WEP Warwick Evans Publishing

Transactions on Social Science, Education and Humanities Research
ISSN: 2960-1770, eISSN: 2960-2262 | Volume 12
LHPPR 2024

Privacy Protection in the Digital Age: Challenges and Strategies

Yuejia Qu

Dongguan University of Technology, Dongguan City, 523808, China

2021280212@emai.szu.edu.cn

Abstract. In today's era of rapid digitalization, the protection of privacy faces serious challenges. This article comprehensively analyzes the main threats to privacy rights in the digital age, including the risks of information leakage brought about by technological advancements, the influence of social culture on the concept of privacy, and the lag in law and ethics in adapting to new technologies. Furthermore, the paper compares the privacy protection legal frameworks of different regions, such as the European Union's GDPR, the United States' CCPA, and China's PIPL, and demonstrates the application and challenges of each legal framework through specific cases. In terms of proposing solutions, the article suggests strengthening the protection of privacy rights from three aspects: legal, technological, and social education. Specific measures include refining relevant laws and regulations, enhancing legal enforcement and supervision, using encryption and anonymization technologies to protect personal information, and improving public awareness of privacy protection and cybersecurity education. These strategies aim to provide comprehensive support for the protection of individual privacy, addressing the various challenges of the digital age.

Keywords: Digital Technology, Privacy Protection, Legal Framework.

1. Introduction

With the rapid development of science and technology, human society has entered a new era - the digital age. Promoted by the international community and various countries, big data and information technology are widely used, penetrating every corner of human life and bringing about significant impact on the development of human society. Digital technology is like a double-edged sword. On one hand, it greatly promotes social progress, changes traditional ways of life, and enhances the convenience of people's lives; on the other hand, as personal information is extensively collected, stored, and utilized, there are many potential issues and dangers in the use and safeguarding of this information. The protection of privacy rights has also become an increasingly important focus of today's society.

Against this backdrop, reinforcing privacy protection holds significant theoretical and practical significance. Firstly, privacy rights are an important component of individual rights, underpinning personal dignity, freedom, and security. In a free society, privacy rights serve as a crucial defense against undue interference, whether from government entities or other public powers. The infringement of these rights can lead to a diminution of individual autonomy, effectively undermining the essence of personal freedom. Moreover, the digital age has introduced a new dimension to privacy concerns, characterized by the enduring nature of digital information and its potential for limitless dissemination. As a result, breaches of privacy can have far-reaching and severe implications for individuals, surpassing the consequences seen in pre-digital eras. Therefore, safeguarding privacy rights is not only a matter of protecting individual interests but also a fundamental requirement for maintaining the integrity and vitality of free societies.

This paper is structured to address three key areas of focus: the challenges to privacy rights presented by the digital age, a comparative analysis of legal frameworks for privacy protection across different jurisdictions, and the formulation of effective strategies and solutions to enhance privacy safeguards. Through a meticulous examination of existing laws and a review of pertinent case studies, the paper aims to elucidate the complex landscape of privacy rights in the digital era. By identifying gaps in current legal protections and proposing actionable solutions, this research endeavors to contribute to

the ongoing discourse on privacy rights, advocating for a more secure and privacy-respecting digital environment. The ultimate goal is to advance the understanding of privacy protection in the digital age, fostering a balanced approach that embraces technological progress while steadfastly protecting individual privacy rights.

2. The Challenges of Privacy Rights in the Digital Era

2.1. Technological Development and Threats to Privacy Rights

Big Data and Personal Information Leakage. Privacy rights, alongside rights such as the right to life, the right to one's name, and the right to reputation, are considered fundamental human rights. In the era of prevalent big data, various kinds of information are digitized and stored in networks, including personal information collected through big data analysis and stored in information databases. Governments, businesses, and institutions have the ability to collect and analyze large amounts of personal information through various means. For instance, many apps require users to provide detailed personal information during registration, which helps strengthen the platform's supervision of users. During the pandemic, the Chinese government required all citizens to report personal information and implemented monitoring of citizens' movements, which provided precise data for pandemic prevention and control, making the efforts more accurate and efficient to a certain extent. However, this collection of information also comes with risks and drawbacks. The collection and usage of data by numerous platforms and entities often exceed the anticipations and consent of users or fall short of regulatory compliance, amplifying the risks associated with personal data breaches. Such incidents can inflict irreparable harm on individuals’ reputations and mental health, lead to financial losses, and erode public trust.

Artificial Intelligence and Abuse of Privacy Information. With the prevalence of big data, artificial intelligence (AI) is also gradually being widely applied in daily life. AI systems rely on vast amounts of data, making the collection and analysis of personal information the foundation of AI system development and application. However, this also opens up possibilities for the misuse of privacy information. While AI technology enhances convenience in daily life, it can also be used for improper monitoring and analysis, infringing upon personal privacy. For example, AI-based facial recognition technology can be used to enhance public safety but may also be utilized for indiscriminate surveillance, violating citizens' privacy rights and freedoms. Furthermore, the operations of AI systems often lack transparency and accountability, obscuring the mechanisms of data collection and usage from users and hindering their ability to manage their private information effectively.

Privacy Security Issues of Internet of Things Devices. The Internet of Things technology (IoT) connects personal or household devices to the internet, greatly enhancing the level of intelligence in daily life. From smart thermostats that adjust temperatures based on user behavior to wearable fitness trackers that monitor health metrics, IoT devices have become integral components of modern living. IoT devices are inherently designed to gather detailed information on user behaviors, preferences, and even physical conditions, creating rich profiles that can enhance user experience through personalized services. Yet, this functionality also opens up avenues for privacy intrusions. The extensive data harvested by IoT devices, ranging from personal health records to real-time location data, becomes a goldmine for entities interested in exploiting this information for unauthorized purposes. Furthermore, the interconnected nature of IoT ecosystems means that a vulnerability in one device can potentially compromise the security of the entire network, leading to widespread data breaches.

2.2. The Impact of Social and Cultural Factors on Privacy Rights

The Change in Public Awareness of Privacy. With the rapid development of information technology, the public's understanding and attitudes toward privacy rights are constantly changing. As incidents of personal information leakage occur frequently, the public's concern for privacy rights is gradually increasing. However, in the digital age, people are increasingly reliant on the internet for daily

communication and information sharing. The convenience of online platforms encourages users to share more personal information. Nevertheless, the process of information collection and usage lacks sufficient transparency and involves hidden breaches. There are technical barriers, which to a certain extent, reduce people's vigilance towards the protection of personal information and weaken users' control over their own information.

The Balance Between Social Surveillance and Privacy Rights. In order to maintain public safety, social surveillance is gradually becoming more prevalent, but inevitably raises issues related to individual privacy rights. Finding a reasonable balance between social surveillance and individual privacy rights is an important challenge facing society today. Some degree of social surveillance is necessary to prevent and combat crime and ensure public safety. For example, video surveillance in public places can effectively deter criminal activities and enhance public safety. However, excessive surveillance may encroach upon individual privacy, infringing upon citizens' rights. For instance, surveillance in areas such as restrooms and private spaces is prohibited. Therefore, it is essential to establish strict regulatory mechanisms to ensure the legality and necessity of surveillance methods.

Cultural Differences and Privacy Rights Protection. The expansion of social surveillance in the quest for public safety introduces intricate challenges to privacy rights. Striking a delicate balance between the needs of social surveillance and the sanctity of individual privacy rights has emerged as a pivotal societal quandary. While a measure of surveillance is deemed essential for deterring criminal activity, safeguarding public safety, and facilitating crime prevention, it's imperative to delineate its bounds carefully. For example, the differences between Chinese and Western cultures serve as a classic illustration. China operates under a predominantly state-owned economic system with strong collectivist ideologies. Therefore, the emphasis on privacy culture in China typically requires that the enjoyment of privacy rights does not harm the interests of the state or the collective. On the other hand, most Western countries, which are primarily capitalist economies with private ownership, highly value individualism.

2.3. Legal and Ethical Challenges

Legal System Lagging Behind Technological Advancements. The phenomenon of legal systems lagging behind technological advancements is widespread. With the rapid development of technology, the emergence of new technologies has brought about many new issues to society. However, the process of formulating and amending laws is complex and time-consuming. In the face of emerging technologies, the law struggles to anticipate the changes brought about by new technologies, making it difficult to keep pace in a timely manner. As a result, legal provisions are unable to effectively regulate the application and development of new technologies, leading to gray areas and introducing uncertainties and risks in many fields.

Ethical Challenges in Privacy Rights Protection. Technological advancements have made the internet and various social media platforms the mainstream mediums for information dissemination, with traditional media also transitioning and upgrading to align with the online space. The dissemination and reporting behaviors of news media, public accounts, video creators, and others should be subject to boundaries and not arbitrary. Due to the permanent and timeless nature of online communication, any piece of news, a video, or a Weibo post has the potential to attract significant social attention at any given moment. This can have a profound impact on individuals whose information is recorded online. Reporters or organizations must balance economic benefits, ethical values, and legal responsibilities, ensuring a complete and factual record of events, rejecting out-of-context information and distortion of facts. Measures such as anonymizing individuals in images or removing personal data are necessary steps to reconcile the exercise of rights with the assumption of responsibilities, thereby upholding the integrity of privacy protection in the digital age.

3. Comparative Analysis of Legal Frameworks for Privacy Protection Internationally

3.1. General Data Protection Regulation

The General Data Protection Regulation (GDPR) of the European Union is a significant component of EU human rights law and privacy law. It was adopted by the European Parliament and the European Council on April 14, 2016, and came into effect on May 25, 2018. The GDPR primarily addresses the strengthening of data subjects' rights, increasing the responsibilities of data processors, regulating cross-border data transfers, and imposing substantial fines for non-compliance. In terms of principles regarding the processing of personal data (Article 5), the GDPR emphasizes principles such as "lawfulness, fairness, and transparency," "purpose limitation," "data minimization," "accuracy," "storage limitation," and "integrity and confidentiality" of data processing, as well as the accountability of controllers' responsibilities and obligations [1].The regulation aims to enhance and harmonize the protection of data provided by all individuals within the European Union and the European Economic Area, profoundly impacting businesses worldwide that handle data of EU citizens. Given the widespread use of the internet globally and the prevalence of privacy concerns in nearly all services, GDPR has implications beyond the EU, influencing legislation in other countries and serving as a model for their regulatory frameworks.

The impact of GDPR on enterprises is profound, requiring businesses to not only reassess and adjust their data processing procedures but also to enhance transparency to ensure full respect for the rights of data subjects. These efforts entail increased operational costs for enterprises. Moreover, GDPR penalties are stringent, and in the event of a data breach, small and medium-sized enterprises lack robust risk resilience, potentially facing severe consequences in the form of hefty fines.

Following the implementation of GDPR, there have been notable cases of companies investigated and fined for violations of its provisions, with Facebook and Google, two tech giants, being particularly noteworthy examples. Meta (formerly Facebook) transferred data from its EU users to servers in the United States. Despite using SCCs and supplementary measures for the transfer, it was found to violate Article 46(1) of the GDPR due to the transfer occurring in a situation where it could not ensure a level of protection essentially equivalent to that in the EU. As a result, it was unable to avail itself of the exception to the transfer prohibition and was fined hundreds of millions of euros by the Irish Data Protection Commission (DPC) [2].

Google's case centered on the opacity of its advertising system, particularly concerning how it processes and utilizes user data for personalized advertising. Following an investigation, Google was found to have insufficiently clear and transparent methods for obtaining "consent" from data subjects before processing personal data for advertising purposes, thereby preventing consumers from giving informed and voluntary "consent," which contravenes GDPR provisions regarding transparency and data subject rights. Consequently, the French data protection authority, CNIL, imposed a fine of €50 million on Google [3].

3.2. California Consumer Privacy Act

The EU's General Data Protection Regulation (GDPR) and incidents like the 2018 Facebook-Cambridge Analytica scandal heightened public awareness of data privacy. In response, California enacted the California Consumer Privacy Act (CCPA) on January 1, 2020, to protect the privacy rights of its residents and regulate consumer data. The CCPA allows consumers to know, access, delete, and opt-out of the sale of their personal information, requiring businesses to disclose data collection and usage practices [4]. As time has passed and privacy regulations have evolved, the CPRA (California Privacy Rights Act) has replaced the CCPA, bringing a series of stricter and clearer provisions, strengthening explicit guidance and obligations for businesses [5].This aims to better protect consumer privacy rights and adapt to an increasingly complex and sensitive data environment. However, during the transition period, the CCPA continues to be enforced, marking a historic leap forward in local privacy protection laws.

While both the CCPA and GDPR aim to protect privacy, they differ due to their national contexts. The GDPR focuses more on individual rights and applies to entities handling EU citizens' data, regardless of location, with stricter compliance and higher fines. In contrast, the CCPA, targeting businesses in California meeting certain revenue criteria, places more emphasis on consumer perspectives and business development. It extends additional rights, such as non-discrimination and protections for minors. The CCPA's penalties are also more lenient, primarily enforced by the California Attorney General's Office.

California's first CCPA enforcement and settlement reached case offers an example of the implementation of CCPA. The California Attorney General accused Sephora of failing to disclose its sale of consumers' personal information, failing to comply with requests to opt-out of sales through user-enabled global privacy controls, and failing to correct these violations within the law's mandated 30-day period. As a result, Sephora will pay a fine of $1.2 million and fulfill a series of compliance obligations [6]. This case emphasizes the critical importance for businesses operating in California to thoroughly understand and comply with the CCPA. Enterprises need to invest in data management and protection technologies, update privacy policies, and train employees to understand and enforce these policies. Additionally, another challenge that businesses face is the redesign of data processing workflows. Enterprises not only need to ensure that the personal information they collect complies with legal requirements but also need to establish effective mechanisms to respond to consumer requests to exercise their rights, such as accessing, deleting, or opting out of the sale of their personal information.

While CCPA presents challenges for businesses, it holds significant importance in protecting consumer rights. By granting consumers greater control, CCPA strengthens the protection of individual privacy. Consumers can now more easily understand how businesses collect, use, and share their personal information, and they can request businesses to delete their information or stop selling it. This not only enhances the level of consumer rights protection but also drives improvements in data processing and privacy protection for businesses, creating a safer, more transparent, and fairer digital environment for both businesses and consumers.

3.3. Personal Information Protection Law

The Personal Information Protection Law (PIPL) of China officially came into effect on November 1, 2021, marking a significant step forward in China's personal data protection efforts. The key provisions of PIPL include principles and rules for processing personal information, responsibilities and obligations of personal information processors, rights of individuals, duties of regulatory authorities, and cross-border data transfers [7]. Compared to the GDPR, PIPL demonstrates efforts to align with international data protection standards in many aspects. Both emphasize the principles of legality and transparency in the processing of personal information, establish rights of data subjects such as the right to access and the right to deletion. Additionally, both PIPL and GDPR require ensuring the security of data during cross-border data transfers. However, PIPL has its own specific measures, such as specific responsibilities imposed on data processors and special provisions for operators of critical information infrastructure within China, reflecting the unique social and legal environment of China.

One notable enforcement under PIPL involved CNKI (China National Knowledge Infrastructure), a major digital repository in China. CNKI stores a vast amount of personal and sensitive information, making it a prime target for overseas hackers. Consequently, the Cyberspace Administration of China conducted a cybersecurity review of CNKI and found it engaged in unlawful handling of personal information. Fourteen apps operated by CNKI were found to have violated PIPL and related regulations by collecting personal information without necessary consent, failing to disclose or specify collection and usage rules, lacking an account cancellation feature, and not promptly deleting users' personal information upon account cancellation. Based on PIPL and other relevant laws and regulations, the National Cyberspace Administration issued an administrative penalty decision for cybersecurity review, ordering CNKI to cease its illegal handling of personal information and

imposing a fine of 50 million RMB [8]. The exposure of this case had a profound impact on society, reminding all enterprises of the necessity to strictly comply with PIPL regulations, enhance awareness of personal information protection, and deepen public understanding of data rights.

In another typical case, Mr. Luo began exploiting opportunities to profit from customer service in gaming and gambling platforms in November 2019 by collecting personal information of citizens. He contacted an individual online and downloaded a large amount of citizen information, including educational records and ID numbers, from a Baidu cloud drive, storing it on his laptop. Subsequently, he illegally sold this information through platforms such as QQ and WeChat, making a total profit of 70,900 RMB. Upon audit and review, it was determined that Mr. Luo had stored a total of 3,471,457 valid data entries. According to Article 10 of the PIPL, "No organization or individual shall illegally collect, use, process, or transmit others' personal information, nor engage in the illegal buying, selling, providing, or disclosing of others' personal information." The court found Mr. Luo guilty of infringing upon citizens' personal information and held him criminally liable. Additionally, through civil public interest litigation, the court ruled for the perpetrator to apologize, compensate for damages, and undertake civil liabilities [9]. This demonstrates that PIPL provides legal protection for individuals' privacy rights and showcases the severe repercussions of illegal handling of personal information, effectively deterring potential violations and strengthening public confidence in personal information protection.

PIPL has significantly strengthened the protection of individual privacy rights, but still faces a series of challenges. Firstly, due to the rapid pace of technological innovation, the law often lags behind technological advancements, resulting in an inability to predict and address emerging issues promptly or resolve conflicts between technology and the law. Secondly, regulatory issues concerning cross-border data transfer are becoming increasingly prominent. In the context of globalization, cross-border data flows have become commonplace, but issues such as jurisdiction, legal conflicts, and legal effectiveness pose significant challenges to data protection. Additionally, inadequate public awareness of personal information protection presents a challenge. A lack of understanding of one's rights makes it difficult for individuals to recognize instances of infringement, thereby diminishing the effectiveness of PIPL implementation to some extent. Despite these shortcomings, the enactment of this law provides a legal foundation for individuals to assert their rights. Therefore, enhancing legal education and utilization remains an ongoing goal.

4. Solutions and Strategies of Privacy Protection in the Digital Age

4.1. Legal Countermeasures

As a crucial boundary for privacy protection, the law possesses binding force and serves as a solid backbone for safeguarding personal information data. Enhancing the establishment of laws concerning personal data privacy protection is imperative. Taking cues from the EU's GDPR, countries should formulate or update data protection laws that align with their national conditions. These laws should clearly define the scope of application and the rights of data subjects, as well as outline the responsibilities and obligations of data collectors. When legislating, attention should be paid to the legal regulation of cross-border data flows. In the era of globalization, cross-border data transfer is commonplace. Therefore, it is essential to strengthen the internationalization of laws, elevate legislative standards, and establish unified or mutually recognized data protection standards. This approach aims to minimize barriers and obstacles to data crossing borders, thereby safeguarding individual privacy from being constrained by national boundaries.

Due to the ubiquity and extensive nature of the internet, enforcing laws and regulations and supervising the flow of network data is a vast and complex endeavor. Firstly, establishing independent regulatory bodies with clear delineations of responsibilities is crucial to comprehensively implement regulatory enforcement efforts and reduce occurrences of corruption. Secondly, increasing the severity of penalties and raising the cost of non-compliance are essential. Sufficiently heavy legal

sanctions, including but not limited to financial penalties, business restrictions, and even criminal liability, should be imposed on actions infringing upon individual privacy rights to enhance compliance with privacy protection regulations. Subsequently, implementing data classification and adopting varying degrees of supervision based on different levels of data can enhance law enforcement efficiency and reduce enforcement costs. Lastly, strengthening international cooperation and enhancing supervision of international data flows are imperative. Establishing international data protection standards and regulatory mechanisms and collectively combating transnational privacy infringements are essential goals.

4.2. Technological Means

Different countries have varying understandings and detailed requirements regarding the anonymization of information. However, the core concept involves using technological means to conceal the privacy information of data subjects, rendering the data untraceable to specific individuals. This technology finds extensive applications in fields such as big data analysis and public research. Using research in the European Union as a benchmark, the development of this technology has progressed from an emphasis on individual privacy protection to discussions on its effectiveness initiated by the EU's Opinion on Anonymization Techniques, and finally to addressing data re-identification issues at both legal and technological levels following the enactment of the GDPR. This progression reflects the integration of anonymization theory and practice.

From a technological standpoint, anonymization techniques primarily include technical aggregation, the addition of data noise, and differential privacy. These methods involve separating or modifying the correlation between data and specific individuals, making it impossible to link the data to particular data subjects [10]. Sensitive information undergoes de-identification, such as replacing direct identifiers like names and phone numbers with non-identifying codes or symbols. Additionally, data confusion can be introduced during sorting, preventing direct associations between published data and the original dataset.

4.3. Social Education and Public Awareness

Enhancing public awareness of privacy protection is the final step in safeguarding personal information. This not only involves disseminating basic knowledge of privacy protection but, more importantly, cultivating habits and abilities among the public to protect privacy in daily life.

The development of the internet, accompanied by emerging technologies and issues, has led to widespread incidents of personal privacy infringement caused by the internet. Most people lack an understanding of the concept of individual privacy rights and methods for safeguarding and asserting their rights regarding personal privacy data. Preventing and addressing this issue requires not only legal and technological advancements but also popularizing the concept of individual privacy among the general public. Therefore, it is essential to disseminate legal information about privacy rights and raise awareness among the public through various means and channels. For example, through media, communities, and other channels, common online fraud methods, laws and regulations on personal information protection, how to set complex passwords, refraining from easily disclosing personal information, and managing application permissions should be popularized.

Adolescents, being the primary demographic engaged in online activities, are also highly susceptible to online risks. Strengthening cybersecurity education for adolescents is crucial for enhancing the overall information security level of society. This includes implementing cybersecurity education courses in schools, conducting cybersecurity-themed activities, enhancing collaboration between families and schools, and guiding adolescents to use the internet in a healthy manner.

5. Conclusion

In the era of big data, the application of technologies such as big data and artificial intelligence has brought many conveniences but has also created new problems. Citizens' personal information is

more easily collected and analyzed, while social and cultural factors and the lag in legal ethics exacerbate this issue. For example, insufficient social awareness of privacy rights and the weak adaptability of existing laws to emerging technologies have placed individual privacy protection in a dilemma. A comparison of important legal frameworks such as the GDPR in the European Union, the CCPA in the United States, and the PIPL in China shows that countries attach great importance to the protection of privacy issues in laws. The implementation of laws has significantly increased the sense of responsibility of enterprises and organizations in handling personal information and enhanced public awareness of privacy protection. However, the perfection and implementation of legal provisions still need to be further strengthened. In addition to updating laws to cover emerging technologies, it is also necessary to enhance law enforcement efforts to ensure effective implementation of the laws. On the technological front, the application of encryption technology and anonymization techniques is an important means to protect the security of personal information. These technologies can effectively prevent unauthorized access to and misuse of data. Furthermore, raising public awareness of privacy protection is also crucial.

In summary, in the face of the protection of individual privacy rights in the digital age, it is necessary to adopt multi-faceted strategies, including but not limited to legal, technological, and educational aspects, to build a secure, healthy, and trustworthy digital society. Globally, enhancing cross-border cooperation, sharing best practices and experiences, is also an important way to promote the development of global privacy protection. Future privacy protection work requires the joint efforts and sustained attention of everyone.

References

[1] European Parliament, Council of the European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Official Journal of the European Union, OJ L 119, 4.5.2016, pp. 1tion work requires the joint effora.eu/eli/reg/2016/679/oj, last accessed 2024/4/6

[2] Melles, C., Kohn, B.: Rekordbußgeld in Höhe von 1,2 Milliarden Euro für Facebook-Mutter Meta Platforms Inc. 22. Mai 2023. Available at: https://www.taylorwessing.com/de/insights-and-events/insights/2023/05/newsflash-rekordbussgeld-fuer-meta

[3] Brook, C.: Google Fined $57M by Data Protection Watchdog Over GDPR Violations. Retrieved from https://www.digitalguardian.com/blog/google-fined-57m-data-protection-watchdog-over-gdpr-violations

[4] Orrick, Herrington & Sutcliffe LLP: CPRA Solutions. Available at: https://www.orrick.com/Solutions/CPRA?__cf_chl_tk=TbiCaoKO4eVfvOkhva1JDq7VB_wTLnJkzhpY2FFoYTc-1713191730-0.0.1.1-1599,last accessed 2024/4/11.

[5] California State Legislature: California Consumer Privacy Act (CCPA). Effective date: January 1, 2020.

[6] Bonta, A.G.: Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act. Wednesday, August 24, 2022. Available at: https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement, last accessed 2024/4/6.

[7] Standing Committee of the National People's Congress: Personal Information Protection Law of the People's Republic of China. Effective date: 11-01-2021.

[8] PKULAW,https://www.pkulaw.com/lar/847ae1a7ce6df4d2da4c000ad04fadfabdfb.html?tiao=1&keyword=Republic of China. Eff,last accessed 2024/4/11.

[9] Office of the Central Cyberspace Affairs Commission: Administrative Review of Network Security by the National Internet Information Office of CNKI in Accordance with the Law. Retrieved from https://www.cac.gov.cn/2023-09/06/c_1695654024248502.htm

[10] Jingwu Zhao. Theoretical Basis and Institutional Construction of Personal Information Anonymization. Chinese and Foreign Law Studies, 36(02), 326-345 (2024).