Advances in Social Behavior Research (2024) Volume 8 EWA Publishing
Published online: 5 June 2024 DOI: 10.54254/2753-7102/8/2024066

The Shield of Privacy in the Digital Age: The Clash between Facial Recognition Technology and Personal Information Protection—Case Analysis and Strategy Discussion

Jingdan Zhang

Bazhong City, Sichuan Province, 636000

2109264591@qq.com

Abstract. Driven by the wave of digitalization, facial recognition technology has become a key tool for identity verification and security monitoring. However, with its widespread application in daily life, issues of personal privacy security have also become prominent. This study delves into the complexities of facial recognition technology in the realm of personal information security through case analysis, revealing its convenience as an identity verification tool and the risks it poses as a potential means of privacy infringement. The research aims to identify and analyze the ethical and legal issues faced by facial recognition technology and to propose strategies for strengthening personal information protection. This paper integrates literature review, case studies, and international comparative analysis to provide support and recommendations for the practice and policy-making of personal information protection in the digital age.

Keywords: Facial recognition, Privacy protection, Strategy development

1. Introduction

In the wave of informatization in the 21st century, facial recognition technology has become a key driver of social progress and economic development. The rapid advancement of this technology has made the collection, storage, and analysis of personal facial data increasingly common, facilitating the provision of personalized services and providing robust technical support for security monitoring. However, this trend has also brought unprecedented challenges to personal privacy rights. Incidents of facial data breaches and misuse have become frequent, raising public concerns about the protection of facial information rights. This study aims to explore the importance and urgency of protecting personal facial information rights in the context of the widespread application of facial recognition technology, and how to construct an effective mechanism for facial information rights protection in a globalized context.

This paper will deeply analyze the current status, challenges, and future directions of facial information rights protection from multiple dimensions, including legal, technical, and international cooperation aspects. The research questions arise from a deep reflection on the current status of facial information rights protection, aiming to address the balance between the free flow of facial information and the protection of personal privacy rights in the era of big data, evaluate the adequacy of the current legal framework, discuss the impact of technological advancements on the protection of facial information rights, and explore how China should construct effective facial information protection strategies on the international stage. Through in-depth discussion and hypothesis testing of these issues, this paper hopes to provide new perspectives and solutions for facial information rights protection and offer theoretical support for the formulation and implementation of related policies. The research findings will help guide policymakers in updating laws and policies to address the new challenges brought by technological developments, while also promoting international cooperation to jointly enhance the global protection level of facial information rights.

The main content and structure of this paper are as follows:

Part One: Review of Research on Facial Recognition and Personal Information Protection. This section reviews the current state of research on facial recognition technology and personal information protection from both international and domestic perspectives and provides a critical assessment.

Part Two: Overview of Facial Recognition Technology. This section explores the development background and application scope of facial recognition technology, analyzes its key role in identity verification and security monitoring, and provides a detailed

introduction to the main application scenarios and social impacts of facial recognition technology. It also discusses the privacy challenges posed by facial recognition technology.

Part Three: Legal Protection and Technical Challenges. This section reviews the legal provisions for personal information protection at both international and domestic levels, such as the Civil Code and the Personal Information Protection Law, focusing on their protection of personal privacy rights. Through case analysis, it explores the impact of the widespread application of facial recognition technology on personal information rights.

Part Four: User Perspective and Social Acceptance. This section discusses the varying attitudes of society towards facial recognition technology, including user concerns about privacy rights and expectations for technological innovation. It highlights the importance of considering personal information security while pursuing technological advancements.

Part Five: International Cooperation and Policy Recommendations. This section analyzes the approaches of different countries in the application of facial recognition technology and personal information protection, as well as the differences between Chinese legal provisions and international standards in this field. It emphasizes the crucial role of international cooperation in promoting personal information protection and proposes specific suggestions for improving the protection of personal information rights.

Part Six: Conclusion. This section summarizes the main findings from the case analyses, offers recommendations for enhancing the protection of personal information rights, and outlines the limitations of the study and future directions.

The objective of this study is to explore how to find a balance between technological innovation and personal information protection by analyzing the conflict between facial recognition technology and personal privacy rights. The primary research methods include literature analysis and case study. By analyzing and comparing relevant legal documents, judicial interpretations, and judicial practices, combined with specific cases, this paper systematically examines the privacy risks of facial recognition technology. The research findings focus on the privacy risks of facial recognition technology, user perspectives, international cooperation, and policy recommendations. These findings provide new perspectives and insights for the healthy development of facial recognition technology and the effective protection of personal information rights. Additionally, the paper identifies the study's limitations and future directions, including the need for deeper legal research on facial recognition technology and personal information protection, and the exploration of further possibilities for international cooperation. It aims to offer theoretical support and practical guidance for the healthy development of facial recognition technology and the effective protection of personal information rights.

2. Review of Research on Facial Recognition and Personal Information Protection

Facial recognition technology and personal information protection is a field full of challenges and opportunities, encompassing aspects such as privacy rights, legal regulations, and technological advancements. This section reviews the current state of research in this field both domestically and internationally.

2.1. International Research Status

Internationally, research on facial recognition technology and personal information protection primarily focuses on the protection of privacy rights and the establishment of legal frameworks. In global studies, European scholars particularly emphasize protecting privacy rights through the implementation of the General Data Protection Regulation (GDPR), which provides a stringent legal framework for personal information protection. American scholars focus on privacy rights protection, exploring how to balance technological utilization with privacy rights through legal regulation.

Renowned scholar Bruce Schneier discusses in his book "Data and Goliath" how big data and surveillance behaviors impact personal privacy, pointing out that the invasion of personal information privacy by facial recognition technology is inevitable, and highlights the necessity of strengthening regulation and legal protection (Bruce Schneier, 2015)[1]. Helen Nissenbaum, a professor of Information Science at Cornell Law School, proposes the "contextual integrity theory," a theory known as the "theory of contextual integrity," which aims to address the challenges posed by technology by proposing a morally nuanced concept of privacy and delineating the boundaries of privacy. She argues that privacy rights should vary with different social and cultural contexts and need to be reasonably balanced in different situations (Helen Nissenbaum, 2021)[2]. Luciano Floridi, a pioneer in the field of information ethics, proposes the "principle of fair information," emphasizing that the acquisition and use of information should adhere to the principle of fairness, without excessively infringing on personal privacy (Luciano Floridi, 2015)[3]. Scholar Daniel J. Solove proposes the "regulation and compliance theory," advocating for the protection of personal information privacy through reasonable regulation and the establishment of relevant legal protective measures (Daniel J. Solove, 2022)[4].

[1] Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.

[2] Beijing University Law School. (2021). Research on Face Recognition Technology and Personal Information Protection [J/OL]. Beijing University Law School Official Website. https://www.law.pku.edu.cn/xwzx/xwdt/145004.htm.

[3] Center for Chinese Philosophy Research. (2015). Privacy Theory: Scholar Nissenbaum Proposed the "Contextual Privacy Theory," Emphasizing that the Acquisition and Utilization of Information Should Follow Fair Principles and Not Overly Infringe on Personal Privacy [J/OL]. Center for Chinese Philosophy Research Official Website.

[4] Solove, D. J. (2022, September 8). On the Limitations of Privacy [Lecture]. Peking University Law School "Digital and Rule of Law" Series Forum. Retrieved from Peking University Law School Website https://www.law.pku.edu.cn/xwzx/xwdt/142908.htm.

In terms of social participation and consensus formation, Professor Yasheng Huang deeply discusses facial recognition, privacy, and the differences between China and the United States in this regard, emphasizing that the new issues brought about by technological development require broad social participation and discussion to reach consensus. He believes that in China, where big data and other technologies are rapidly developing, discussions on privacy should be more in-depth (Huang Yasheng, 2022) [5]. Regarding the balance between technological application and privacy rights, Barry Friedman and Andrew Guthrie Ferguson expressed concerns about the use of facial recognition technology by law enforcement agencies in an article published in The New York Times, calling for restrictions on its use to protect citizens' privacy rights (2019) [6]. In terms of global governance and legislative practice, Qingxiu Bu's paper published in the International Cybersecurity Law Review analyzes the legislative and practical experiences of countries like those in Europe and the United States in facial recognition governance and based on this, proposes suggestions for global governance (Bu Qingxiu, 2021) [7].

2.2. Domestic Research Status

Domestic scholars are increasingly delving into the research on facial recognition technology and personal information protection. Chinese law is gradually improving in terms of protecting personal information, particularly with the promulgation of the Civil Code, which provides a clearer legal basis for personal information protection. However, scholars point out that there are systemic inadequacies in the current legal framework for privacy protection in the application of facial recognition technology in China. These include a lack of specific regulatory measures and insufficient regulatory enforcement (Fan Yanru, 2022) [8].

In terms of legal protection and current legislative status, Fan Yanru analyzed the "first face recognition case in Hangzhou" to explore the legal protection of face recognition information under the Civil Code. She proposed case-based legal protection suggestions, emphasizing that laws should be updated in tandem with technological advancements to protect personal privacy (Fan Yanru, 2022) [9]. Gao Zhongshao focused on the sensitive nature of facial recognition information and analyzed the current legislative status of facial recognition information protection in China. He emphasized the need for special legal protections for sensitive information (Gao Zhongshao, 2022) [10]. In the context of consent authorization and individual privacy, Shi Jiayou and Liu Siqi introduced the concept of dynamic consent model, advocating for its implementation to ensure the clarity and effectiveness of consent authorization. They argue that this approach can better adapt to technological advancements and the needs for personal privacy protection (Shi Jiayou & Liu Siqi, 2021)[11]. Regarding the conditions for processing sensitive information, Zhongming Yue discussed the specific provisions in the draft Personal Information Protection Law concerning the handling of sensitive personal information such as facial recognition. He emphasized that processing sensitive personal information should only occur under specific purposes and with sufficient necessity (Yue Zhongming, 2020)[12]. In terms of technological advancements and legal responses, Liu Junping and Yang Zhiqing discussed the challenges of facial recognition data protection and corresponding legal strategies. They addressed the controversies surrounding the development of facial recognition technology and the widespread societal concerns regarding information protection (Liu Junping & Yang Zhiqing, 2021)[13].

To improve the current state of facial recognition technology and personal information protection, scholars have proposed various solutions, including strengthening the legal system, improving specific regulatory measures, enhancing regulatory enforcement, and raising public awareness of legal protections. Additionally, they suggest drawing on international legislative experiences and tailoring regulations to China's specific context to create more detailed and balanced provisions (Jin Xin, 2023) [14].

2.3. Critical Review

The legal protection of facial recognition technology is a complex and evolving field. Scholars' work not only reveals the inadequacies of the existing legal system but also proposes innovative legal concepts and frameworks to adapt to technological

[5] YouTube. (2022). How to Bake the Perfect Chocolate Chip Cookies . https://www.youtube.com/watch?v=qIiG5VaLnWc

[6] Friedman, B., & Ferguson, A. G. (2019). Here's a Way Forward on Facial Recognition. The New York Times. Retrieved from The New York Times website.

[7] Bu, Q. X. (2021). The Global Governance on Automated Facial Recognition (AFR): Ethical and Legal Opportunities and Privacy Challenges. International Cybersecurity Law Review, 2.

[8] Fan, Y. R. (2022). Legal Protection Research on Face Recognition Information in the Perspective of Civil Code—Starting from the "First Case of Face Recognition" in Hangzhou [J]. Dispute Resolution, 8(2), 232-237.

[9] See Reference [8].

[10] Gao, Z. S. (2022). Legal Regulation of Facial Recognition Information Processing Behavior [J]. Learning Forum, (01), 130-136. DOI:10.16133/j.cnki.xxlt.2022.01.017.

[11] Shi, J. Y., & Liu, S. Q. (2021). Protection of Personal Information in Facial Recognition Technology—Discussion on the Construction of Dynamic Consent Model [J]. Financial and Economic Law, 2021(2), 60-78.

[12] National People's Congress. Decision on Strengthening Network Information Protection [DB/OL]. (2020-12-21) [2024-05-03].

[13] Liu, J. P., & Yang, Z. Q. (2021). Privacy Issues Analysis of Facial Recognition Technology and Its Legal Countermeasures [J]. Science and Law (Chinese and English), 2021, (06), 18-28. DOI:10.19685/j.cnki.cn11-2922/n.2021.06.003.

[14] Jin, X. (2023). Making Facial Information More Effectively Protected (People's Comment). People's Daily.

advances and changing societal needs. These studies are crucial for formulating effective legal policies, protecting personal privacy rights, and promoting the harmonious development of technology and law. However, comprehensive analysis reveals several issues in current research: First, current studies often emphasize the legal aspects of facial recognition technology and personal information protection while neglecting an in-depth analysis of technical details, such as the working principles and error rates. Second, there is a lack of comparative research across countries to evaluate the application and regulation under different legal systems. Third, interdisciplinary perspectives integrating law, technology, and ethics are underutilized in studying facial recognition technology and personal information protection. Fourth, empirical research and case studies are relatively insufficient, especially in evaluating the practical effectiveness and issues of the technology. Research on users' cognition, attitudes, and participation levels is also lacking, which is crucial for devising effective privacy protection measures. Fifth, with the rapid development of artificial intelligence and machine learning technologies, existing studies fail to predict the future impact of these advancements on legal protection measures. The policy recommendations proposed lack comprehensive evaluations of implementation difficulty, cost-effectiveness, and socioeconomic impacts. Lastly, research is inadequate in considering the impact of facial recognition technology on specific social groups such as ethnic minorities and children, who require more attention to their privacy rights protection.

In summary, facial recognition technology and personal information protection is an interdisciplinary and multidimensional research field involving law, ethics, technology, and more. Future research needs to further explore how to effectively protect personal privacy rights while promoting technological development. This field of study is not only significant for the legal community but also has profound implications for technological advancement and social governance.

3. Overview of Facial Recognition Technology

Facial recognition technology is a biometric technology that verifies identities based on facial features. It typically involves the following steps: acquiring facial images, detecting facial features, extracting feature data, and matching it with stored facial data in a database. This process involves complex algorithms, including deep learning and neural networks, particularly convolutional neural networks (CNNs), which are crucial components of artificial intelligence. The key characteristics of facial recognition technology include its non-contact nature, ease of deployment, and user-friendliness, making it widely applicable across various fields.

3.1. Main Application Scenarios and Social Impact of Facial Recognition Technology

The extensive application of facial recognition in China has become a significant feature of social development. By automatically processing digital images containing personal faces, it facilitates the identification, verification, or classification of individuals[15]. The primary functions of this technology include verification, identification, and classification. Verification is typically used for identity authentication, such as one-to-one matching during check-in procedures. Identification involves one-to-many comparisons, such as the Tianwang system used by public security agencies to identify criminals. Classification involves analyzing facial features to determine characteristics such as gender, age, and race[16]. The application scenarios of facial recognition technology are incredibly diverse, including but not limited to security and surveillance, personal device security, financial services, and healthcare. In security and surveillance, facial recognition is used in monitoring systems at airports, stations, and urban surveillance networks. In personal device security, it is implemented on personal electronic devices like smartphones and laptops. In financial services, banks and payment platforms use facial recognition to verify customer identities. In healthcare, facial recognition helps doctors remotely verify patient identities to ensure the security of medical information.

[17]Due to its efficiency and convenience, China leads the global development and application of facial recognition technology. However, as the technology becomes more widespread, the security and privacy protection of facial information, a sensitive personal biometric data, have increasingly come under scrutiny. The uniqueness and invariability of facial information mean that if it is leaked or misused, it could pose significant risks to individuals, including financial security and personal privacy. Examples of such risks include illegal loans, fraud, and potential impacts on public safety. Therefore, as facial recognition technology continues to develop, ensuring the security and privacy protection of personal information will be a long-term and crucial task. This requires not only technological innovation to enhance security but also legal and policy support to regulate its use and public education to raise awareness of these issues. Only through such comprehensive measures can facial recognition technology continue to contribute to societal development while safeguarding individual rights.

[15] Cheng, X. (2021). Understanding and Application of Personal Information Protection Law. China Legal Publishing House. 240-241.

[16] Cheng, X. (2021). Understanding and Application of Personal Information Protection Law. China Legal Publishing House. 240-241.

[17] Long, W. Q. (2022). Expert Comments on the First Case of Facial Recognition Dispute. People's Court Daily, Top Ten Cases of People's Court in 2021. Retrieved from People's Court Daily Website: https://www.pkulaw.com

3.2. Privacy Challenges of Facial Recognition Technology

While facial recognition technology provides convenience, it also presents potential risks to personal privacy. Yanru Fan points out in her research that every stage from data collection, storage, to usage can become a risk point for privacy leaks (Fan Yanru, 2022) [18]. Especially in the absence of adequate legal protections and technical security measures, personal facial data might be accessed and misused by unauthorized third parties. Pengyu Jiang further explores the privacy issues of facial recognition technology, emphasizing the threat to personal privacy posed by indiscriminate data collection in public places (Jiang Pengyu, 2023) [19]. Zhijie Zheng and Zixuan Huang analyze the dilemmas of privacy protection in the big data era, highlighting how large-scale data collection and analysis can lead to unintentional disclosure of personal information (Zheng Zhijie & Huang Zixuan, 2023) [20]. The research by Ning He, Yongjin Chen, and Dayong Yang reveals the complexity of privacy issues in the context of big data, noting that the opacity of algorithms and automated decision-making can increase the risk of privacy infringement, while users often lack awareness and control over this (He Ning & Chen Yongjin, 2020) [21].

The relationship between facial recognition technology and personal privacy rights presents a double-edged sword. On one hand, this technology brings great convenience to our lives; on the other hand, it raises serious concerns about personal privacy. The studies by Yanru Fan (2022) and Pengyu Jiang (2023) reveal potential privacy leak risks at each stage of data collection, storage, and usage. Research by Zhijie Zheng and Zixuan Huang (2023), as well as Ning He, Yongjin Chen, and Dayong Yang (2020), emphasize new challenges to privacy protection in the context of big data and artificial intelligence, particularly the potential threats posed by algorithmic opacity and automated decision-making to privacy rights. To address these challenges, a multifaceted strategy is required. First, it is essential to strengthen the legal framework to set clear boundaries for the reasonable use of facial recognition technology. Second, technological innovation should focus on enhancing data security and privacy protection, such as improving encryption technologies and developing more refined user authorization mechanisms. Additionally, public education and awareness are crucial to increase individuals' proactive involvement in data protection. Finally, international cooperation is vital for establishing globally recognized privacy protection standards and rules for cross-border data flow. Through these comprehensive measures, we can enjoy the convenience brought by facial recognition technology while effectively protecting personal privacy rights.

4. Legal Protection and Technological Challenges - The Intersection of Facial Recognition and Personal Privacy Rights

4.1. Legal Provisions for Personal Information Protection at Home and Abroad

At the legal level, the protection of personal information has been covered by multiple legislations. Globally, various legal systems have been established for personal information protection. The European Union's General Data Protection Regulation (GDPR) is one of the most well-known regulations in this regard. It provides strict guiding principles for the processing of personal data, imposes stringent requirements on how businesses handle personal data, and grants extensive rights to data subjects. Its scope is very broad, applying not only to businesses within the EU but also to foreign companies providing goods or services to EU citizens. In contrast, the United States has adopted a more decentralized and industry-specific legal system. For example, the California Consumer Privacy Act (CCPA) enacted in 1974 specifies the responsibilities and obligations of the federal government in information management and personal information protection, providing consumers with control over their personal information, including rights to information, deletion, and objection to the sale of personal information. This act also applies to institutions that collect, store, and process personal information using facial recognition technology. The Data Protection Act in the UK was the data protection law used by the UK before the GDPR came into effect. It established a regulatory framework for data use in the UK, specifying requirements for the processing and protection of personal data, including data generated by the use of facial recognition technology. The Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada ensures the protection of personal information in Canada and sets out the personal data protection principles that organizations need to adhere to, including the application of facial recognition technology.

In China, the legal system has made clear provisions and responses regarding the application and management of facial recognition technology. The Civil Code incorporates facial information and other biometric identification information into the scope of personal information protection, emphasizing legal protection for such sensitive information. [22] The "Personal Information Security Specification (Revised in 2020)" explicitly defines personal biometric information as sensitive information, requiring higher standards of protection when processing such information. The "Personal Information Protection Law" authorizes

[18] See Reference [8].

[19] Jiang, P. Y., & Du, Y. Y. (2023). Analysis of Privacy Issues of Face Recognition Technology [J]. Yunnan Social Sciences, 2023, (04), 63-69.

[20] Zheng, Z. J., & Huang, Z. X. (2023). Dilemmas and Solutions of Privacy Protection in the Big Data Era [J]. Legal Studies (Hans), 11(4), 3035-3040.

[21] He, N., Chen, Y. J., & Yang, D. R. (2020). Research Status and Hotspot Analysis of Privacy Issues in the Background of Big Data—Statistical and Content Analysis Based on 84 Journal Papers [J]. Frontiers of Social Science, 9(10), 1541-1547.

[22] Refer to Articles 1034 and 1035 of the Civil Code.

the Cyberspace Administration of China (CAC) to formulate specific rules and standards for the protection of facial recognition personal information to ensure the security and lawful use of personal information. It further elaborates on the rules and conditions for the processing of personal information, emphasizing the rights of data subjects to be informed and to choose. This law was promulgated on August 20, 2021, and came into effect on November 1 of the same year. It specifies the principles of legality for personal information processing, including the principles of minimization, purpose specification, and openness and transparency. It also stipulates the obligations of personal information processors, such as establishing sound personal information protection systems and adopting corresponding technical measures to ensure the security of personal information. Additionally, it emphasizes the regulation of cross-border data transfers, requiring specific conditions to be met before such transfers, such as security assessments and the signing of data transfer agreements. The "Regulation on the Administration of Internet Data Security (Draft for Solicitation of Comments)" stipulate that data processors should not use biometric characteristics such as facial features, gait, fingerprints, iris, and voiceprint as the sole means of personal identity authentication to prevent excessive infringement of personal privacy and potential security risks[23]. The purpose of this regulation is to standardize network data processing activities, protect the legitimate rights and interests of individuals and organizations in cyberspace, and safeguard national security and public interests. Moreover, this regulation explicitly establishes a data classification and grading protection system, categorizing data into general data, important data, and core data, and applying different protection measures to different levels of data. The "Cybersecurity Law of the People's Republic of China" specifies the provisions that network operators must follow when collecting and using users' personal information to ensure the security and privacy of personal information. The "Criminal Law of the People's Republic of China" clearly defines the criminal responsibility for acts such as infringing on personal information and illegally obtaining personal information. In addition, the Supreme People's Court has issued the world's first judicial interpretation of facial recognition, "Provisions on Several Issues Concerning the Application of Law in the Trial of Civil Cases Involving the Use of Facial Recognition Technology to Process Personal Information," further clarifying the standards and limitations of facial recognition technology in judicial practice, reflecting China's pioneering exploration and legislative practice regarding legal issues related to facial recognition technology on a global scale.

While China's current legal system does not have specific laws for the protection of biometric information, provisions for personal information protection are scattered throughout various legal norms such as the Civil Code, the Consumer Rights Protection Law, and the Cybersecurity Law, which include incorporating biometric information into the scope of personal information. These provisions collectively establish the basic framework for personal information protection, aiming to find a balance between technological advancement and personal privacy rights. Although biometric information has not yet become an independent absolute right, existing laws emphasize the protection of the right of natural persons to control personal information and ensure that individuals can obtain legal remedies when their information is illegally infringed upon.

4.2. Analysis of Legal Cases at Home and Abroad

In today's rapidly developing era of big data and artificial intelligence technology, the right to privacy faces unprecedented challenges. The opacity of algorithms and automated decision-making processes exacerbates the risks of privacy infringement, while most users often lack the necessary understanding and control over these processes. While the use of personal information can promote social welfare, it may also lead to the infringement of the rights and interests of information subjects. Therefore, the protection of personal information becomes particularly important. The legal system must find a balance between broad demands and limited resources to ensure the optimal protection mechanism.

4.2.1. Wide Application of Facial Recognition: Crime of Infringing on Citizens' Personal Information

In Guiding Case No. 192 issued by the Supreme People's Court[24], the defendant Li Kaixiang was prosecuted for developing and selling a hacker software disguised as a "beauty detection" application, illegally obtaining photos from users' albums, including facial information and other personal information. The court determined that facial information belongs to citizens' personal information, and Li Kaixiang's actions constituted the crime of infringing on citizens' personal information. This case emphasizes the highly identifiable nature and social harm of facial information, as well as the criminal responsibility for illegally obtaining facial information.

Regarding whether the facial information illegally obtained by the "beauty detection" software constitutes "citizens' personal information" under the Criminal Law, there are two key points. First, both the facial information processed by facial recognition technology and the facial information generated based on this technology are highly identifiable and thus fall under the Criminal Law's definition of "citizens' personal information". Second, if these pieces of information are obtained through theft or other illegal means, and the circumstances are serious, it constitutes the crime of infringing on citizens' personal information. According to the "Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringing on Citizens'

[23] The Provision 25 of the Regulation on the Administration of Internet Data Security (Draft for Solicitation of Comments) stipulates: "Data processors using biometric features for personal identity authentication shall conduct risk assessments on necessity and security, and shall not use facial, gait, fingerprint, iris, voiceprint, and other biometric features as the sole means of personal identity authentication without the individual's consent to collect their biometric information."

[24] Please refer to (2021) Hu 0120 Xing Chu No. 828.

Personal Information" jointly issued by the Supreme People's Court and the Supreme People's Procuratorate, personal information is divided into three categories: super-sensitive information, sensitive information, and general information. [25]Although Guiding Case No. 192 by the Supreme People's Court does not explicitly specify which category facial information belongs to according to the judicial interpretation, based on the viewpoint of this guiding case, illegally obtaining 5000 pieces of facial information constitutes the crime of infringing on citizens' personal information.[26]

The popularization of facial recognition technology has raised concerns about the potential abuse of public power, such as the surveillance risks depicted in the movie "Enemy of the State" involving big data and artificial intelligence. In China, the government proposed the goal of achieving comprehensive coverage and sharing of the public safety video surveillance network by 2020 in the "Opinions on Strengthening the Construction and Application of Public Security Video Surveillance Networks"[27] issued in 2015. According to statistics, there are approximately one billion official cameras in China's "Skynet" system, with each citizen being captured by cameras over 500 times on average per day[28]. China's "Personal Information Protection Law" stipulates that the installation of image capture and personal identity recognition devices in public places must be necessary for maintaining public safety, and must comply with relevant national regulations, including setting clear warning signs[29]. Furthermore, collected personal images and identity recognition information can only be used for the purpose of maintaining public safety, unless individual consent is obtained. In the education sector, some universities require students to undergo facial recognition during postgraduate entrance exams without providing alternative options. According to the regulations of the Ministry of Education, facial recognition of incoming freshmen is aimed at preventing impersonation. However, the "Personal Information Protection Law" stipulates that obtaining individual consent is required for processing sensitive personal information. These regulations and practices indicate that while facial recognition technology plays an important role in security and verification, strict legal regulations are also necessary to protect citizens' personal information from infringement.[30]

4.2.2. The Widespread Application of Facial Recognition: "The Guo Bing Case"

In April 2021, the widely followed "first facial recognition case" (the Guo Bing case) was announced in its second trial. The main facts of the case are as follows: Guo Bing purchased a dual-person annual pass for the Hangzhou Safari Park, and his relevant personal identity information, including fingerprints and photos, was retained. Subsequently, Hangzhou Safari Park changed the entry method for the annual pass from fingerprint recognition to facial recognition and required Guo Bing to undergo facial activation. Unable to reach a settlement through negotiation, a dispute arose. In the first instance, the Fuyang District Court of Hangzhou ruled that Hangzhou Safari Park should compensate Guo Bing for contractual losses and transportation expenses, and delete Guo Bing's facial feature information submitted when he applied for the annual pass, including the photo, but rejected Guo Bing's other claims[31]. In the second trial, the Hangzhou Intermediate Court held that since the fingerprint recognition turnstile had ceased operation, the originally agreed-upon entry method could not be realized, and therefore Guo Bing's fingerprint recognition

[25] The drafters of judicial interpretations describe "hyper-sensitive information" as "highly sensitive information". See Zhou Jiahai, Zou Tao, Yu Haisong: "Understanding and Application of the Interpretation on Handling Criminal Cases of Infringement of Citizens' Personal Information" in People's Judiciary (Application) 2017 Issue 19, page 34. However, some scholars believe that personal information in judicial interpretations is divided into sensitive information, important information, and general information. See Zhou Guangquan: "The Subjects of the Crime of Infringing on Citizens' Personal Information" in Tsinghua Law Review 2021 Issue 3, page 32. Adopting this classification may lead to excessive expansion of the power to impose penalties. Article 28 of China's Personal Information Protection Law stipulates: "Sensitive personal information refers to personal information that, once leaked or illegally used, is likely to endanger the personal dignity, personal safety, or property security of natural persons, including biometric information, religious beliefs, specific identities, medical and health information, financial accounts, travel trajectories, and personal information of minors under the age of fourteen." In the standards for criminal liability specified in the "Judicial Interpretation on Personal Information", one situation is "illegally obtaining, selling, or providing more than five hundred pieces of citizens' personal information such as accommodation information, communication records, health and physiological information, transaction information, which may affect personal or property safety", and the personal information therein conforms to the definition of sensitive information in Article 28 of the Personal Information Protection Law. Cited from Luo Xiang. On the Limits and Application of Criminal Regulation of Facial Recognition - Taking Guiding Cases of Crimes of Infringement of Citizens' Personal Information as an Entry Point in Comparative Law Research 2023 (2): 17-30 footnote [1].

[26] Luo, X. (2023). On the Limits and Application of Criminal Regulation of Facial Recognition: A Case Study of Crimes of Infringement of Citizens' Personal Information. Comparative Law Research, 2, 17-30.

[27] See National Development and Reform Commission, Central Comprehensive Governance Office, Ministry of Science and Technology, and other opinions on strengthening the application of networked public security video surveillance construction work.

[28] Cheng, X. (2021). Understanding and Application of the Personal Information Protection Law. China Legal Publishing House, p. 242.

[29] Article 26 of the Personal Information Protection Law of the People's Republic of China stipulates: "When installing image acquisition and personal identity recognition devices in public places, it shall be necessary to maintain public safety, comply with relevant national regulations, and set significant warning signs. The collected personal images and identity recognition information shall only be used for the purpose of maintaining public safety and shall not be used for other purposes, except with the individual's separate consent."

[30] Article 29 of the Personal Information Protection Law of the People's Republic of China stipulates: "Sensitive personal information shall be obtained with the individual's separate consent; for the processing of sensitive personal information stipulated by laws and administrative regulations to obtain written consent, comply with their provisions."

[31] See (2019) Zhejiang 0111 Min Chu 6971.

information should also be deleted. [32]The second-instance court upheld the first-instance court's judgment, determining that Hangzhou Safari World's use of Guo Bing's facial recognition information without his consent violated the principle of necessity and ordered the deletion of Guo Bing's fingerprint information.

This case, arising from a service contract dispute caused by the operator's collection and use of consumers' biometric information for identity verification, preliminarily explores the issue of the lawful use of biometric information in the consumer field and explores and attempts to establish rules for the deletion of personal information[33] within the current legal framework[34]. According to the legal provisions in the fourth part of the article, in the consumer field, the legality, legitimacy, and necessity of the behavior of information handlers in processing biometric information should be examined in accordance with the principles of legality, legitimacy, and necessity, and the consent of the parties involved. The principle of legality requires that the collection and processing of personal information must have a legal basis and comply with all legal requirements; legitimacy includes the legitimacy of business and purposes; necessity requires that the collection and use of personal information must not exceed the statutory or agreed scope, achieve the minimum necessary limit for the purpose of collection and use, and be promptly deleted after the purpose is achieved. The rule of informed consent requires that the processing of personal information should explicitly state the purpose, method, and scope of information processing, disclose the rules for processing information, and obtain the consent of the personal information subject or their guardian unless consent is not required by law.

In this case, Hangzhou Safari Park required Guo Bing to activate facial recognition, which exceeded the purpose of prior collection, posing a potential risk to Guo Bing's personal interests in facial feature information. Therefore, the facial feature information submitted by Guo Bing when applying for the card, including the photo, should be deleted. Hangzhou Safari Park's collection and use of Guo Bing's fingerprint recognition information were done with his informed consent. However, given the unilateral change by Hangzhou Safari Park in the entry method for the annual pass from fingerprint recognition to facial recognition during the performance of the contract, and the cessation of the use of fingerprint recognition turnstiles, rendering the originally agreed-upon fingerprint recognition entry service unachievable, the fingerprint recognition information should also be deleted. The first-instance judgment in this case was based on Hangzhou Safari Park's violation of the agreement between the parties in handling the information, resulting in the deletion of facial recognition information. The second-instance judgment, by additionally ordering the deletion of fingerprint recognition information based on the original judgment, further established the judicial rule that information handlers should delete biometric information collected corresponding to the service when they cease to provide the relevant service due to breach of contract, which responded to public expectations to the greatest extent within the current legal framework and played a demonstrative role in similar case adjudication.

4.2.3. Summary

Currently, legislation on the application of facial recognition technology in China is still incomplete, judicial and law enforcement standards are inconsistent, and there are deficiencies in industry self-discipline norms. This has led to a lack of unified consensus on the legal issues involving facial recognition technology. The main controversies focus on two aspects: First, the legal attributes of facial feature information: There are different opinions on whether facial feature information belongs to sensitive personal information and how it should be protected and handled. Second, regulatory requirements for facial recognition applications: Normative requirements for the scope, conditions, and limitations of facial recognition technology applications are not yet clear and require further legal provisions and industry standards for guidance.[35]

4.3. Balancing Law and Technology

4.3.1. Synergistic Development of Technological Innovation and Privacy Protection

Balancing technological innovation and privacy protection requires meticulous legal frameworks and technical solutions. Research by Fan Yanru emphasizes the role of the Civil Code in protecting facial recognition information and proposes that clear legal provisions should be established to prevent the misuse of personal information (Fan Yanru, 2022)[36]. Zhao Jingwu explores the

[32] See (2020) Zhejiang 01 Min Zhong 10940.

[33] The right to be forgotten originates from the European Union, and the concept of this right was first proposed when the European Commission revised the Data Protection Directive in 2012. Currently, Chinese law does not establish the concept of the right to deletion or the right to be forgotten. The Civil Code, the Cybersecurity Law, and other laws provide for deletion in cases of illegal or contractual processing of personal information. During the trial process of this case, Fuyang Court held an expert opinion consultation meeting, where experts believed that the right to deletion should be limited to breaches and illegal situations defined by current laws and should not be expanded. The Personal Information Protection Law also suggests a tendency to expand the right to deletion beyond the aforementioned circumstances, such as when the agreed-upon retention period has expired or the processing purpose has been achieved, or when the personal information processor ceases to provide products or services, or when the individual withdraws consent.

[34] Xu, M., & Han, S. (2021). Caution and Strict Protection of Biometric Information. People's Judiciary, 2021(23), 4-8. DOI:10.19684/j.cnki.1002-4603.2021.23.028.

[35] See Reference [30].

[36] See Reference [8].

issue of the ownership of facial recognition information rights and suggests the establishment of more specific legal provisions to clarify the rights of personal information and protection pathways (Zhao Jingwu, 2020)[37]. These studies indicate that laws should not only protect personal privacy but also promote the reasonable application of technology.

At the legal level, existing legal frameworks should be improved, and specific legal provisions regarding facial recognition technology should be formulated to clarify the boundaries and conditions of data collection, processing, and usage. At the technical level, the development and promotion of Privacy-Enhancing Technologies (PETs), such as anonymization processing and localized computing, should be undertaken to minimize the risk of data leakage. Simultaneously, more refined user authorization mechanisms should be designed to ensure individual informed consent during the process of data collection and usage. At the societal level, public awareness of the right to personal privacy should be enhanced, and individuals' proactive and self-protection capabilities in data protection should be strengthened through education and advocacy activities.

4.3.2. Strategies for Protecting Individual Information Rights in Facial Recognition Technology

In the rapidly developing field of facial recognition technology, ensuring the protection of individual information rights is particularly important. The "Regulations on the Security Management of Facial Recognition Technology Application (Trial) (Draft for Solicitation of Comments)"[38] issued by the Cyberspace Administration of China provide a policy framework aimed at regulating the application of facial recognition technology and ensuring the security of personal information. Additionally, it is suggested to adopt a "multi-level" legal framework to protect facial recognition information, involving legislation, law enforcement, and judiciary aspects, aimed at comprehensively safeguarding individual information rights by formulating specific legal provisions, strengthening the punishment for illegal acts, and providing judicial remedies.

To protect individuals' rights to personal information in facial recognition technology, comprehensive strategies should be adopted. These include embedding privacy protection mechanisms at the development stage to ensure full respect and protection of users' facial data. Setting privacy-friendly default options can reduce the risk of exposing users' facial data. Collaborating with other countries and regions to jointly research and establish rules for cross-border data flows is essential to establish internationally recognized privacy protection standards. Additionally, strengthening regulatory and accountability mechanisms is crucial. Establishing dedicated regulatory bodies to oversee the application of facial recognition technology and ensuring compliance with relevant laws by all technology providers and users are necessary steps. Prompt measures should be taken in case of personal information leakage or misuse, and accountability should be enforced on the responsible parties.

Through concerted efforts across legal, technological, and social dimensions, it should be possible to promote technological innovation while protecting individual privacy rights, ensuring that personal privacy is fully respected and protected in the digitalization process.

5. User Perspectives and Social Ethics

According to a survey conducted by the Social Survey Center of the China Youth Daily in collaboration with a questionnaire website, more than half of the respondents have doubts about facial recognition technology, fearing personal information leakage and theft. Additionally, the "Public Survey Report on Facial Recognition Applications (2020)" reveals public concerns about the trend of abuse of facial recognition technology, as well as cases of privacy or property loss due to facial information leakage and abuse.

The ethical challenges of facial recognition technology are also a significant concern. Reports in Nature magazine explore the ethical considerations behind facial recognition systems, including the analysis by scientists of the inherent inaccuracies and biases of facial recognition technology, as well as warnings about discrimination and calls for increased regulation and transparency in technology. Experts caution against the misuse of facial recognition technology and emphasize the importance of protecting personal information security, highlighting the importance of regulatory mechanisms and accountability for the application of facial recognition technology.

6. International Cooperation and Policy Recommendations

On a global scale, different countries have adopted diverse laws and policies regarding the application of facial recognition technology and the protection of personal information. The General Data Protection Regulation (GDPR)[39] established by the European Union sets strict principles for data processing and high standards for the protection of individual privacy rights, emphasizing data minimization and transparency. While the United States does not have a unified federal privacy law, state laws

[37] Zhao, J. (2020). Attribution and Protection Path of Facial Recognition Information under the Vision of the Civil Code. Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition), 33(5), 21-29.

[38] State Internet Information Office. (August 8, 2023). Draft for Solicitation of Opinions on the Safe Management Regulations for the Application of Facial Recognition Technology.

[39] European Parliament and Council of the European Union. (2016). 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). Official Journal of the European Union, L 119, 1-88.

such as the California Consumer Privacy Act (CCPA)[40] and the upcoming California Privacy Rights Act (CPRA)[41] provide consumers with more control and transparency. Asian countries such as Japa[42]n and South Korea[43] have also strengthened the protection of personal information through legislation to ensure the legality and security of data processing.

The Personal Information Protection Law (PIPL) promulgated in China in 2021 is an important supplement to the field of personal information protection, marking significant progress in Chinese legislation for personal information protection. To some extent, it aligns with international standards by emphasizing the legality, legitimacy, and necessity of data processing. However, compared to international standards like GDPR, PIPL still has gaps in the enforcement of data subject rights protection, regulation of cross-border data flows, exercise of individual rights, provisions on cross-border data transfers, and establishment of regulatory mechanisms. PIPL defines the obligations and responsibilities of data processors broadly, and its provisions regarding cross-border data transfer and data subject's rights to information and choice are relatively vague. Furthermore, it lacks clear guidance and standards for regulating international data flows.

To better promote the protection of personal information, the importance of international cooperation is increasingly prominent. By joining international organizations and signing multilateral agreements, countries can collaborate to formulate and adhere to international guidelines for data protection. This not only helps to establish unified standards for data protection but also facilitates secure cross-border data flow. For example, the Cross-Border Privacy Rules System (CBPR) under the Asia-Pacific Economic Cooperation (APEC) serves as an effective mechanism for promoting data flow within the region. China actively participates in CBPR and the Global Privacy Alliance (GPA) and exchanges best practices with other countries, which is crucial for strengthening law enforcement domestically, enhancing transparency in data processing, and improving mechanisms for the exercise of personal rights. Additionally, China should increase investment in the enforcement of the Personal Information Protection Law (PIPL), clarify the responsibilities of data processors, and strengthen the regulation of cross-border data flows to ensure the security of personal information.

On a global scale, countries have different approaches to the application and regulation of facial recognition technology. Some countries have established strict privacy protection regulations, while others prioritize technological development and application. By comparing the practices of different countries, a deeper understanding can be gained of how to strike an appropriate balance between safeguarding privacy rights and promoting technological innovation. This balance is crucial for ensuring technological progress while protecting the rights of citizens.

7. Conclusion

This paper, through an in-depth analysis of facial recognition technology and the protection of personal information, reveals the complex relationship between the convenience and privacy risks brought about by this technology in the digital age. The research indicates that while facial recognition technology provides important tools for identity verification and security monitoring, its widespread application has also raised serious concerns about individual privacy and security. The core of this study lies in identifying and analyzing the ethical and legal issues faced by facial recognition technology and proposing a series of strategies to enhance the protection of personal information.

7.1. Innovations, Insights, or Managerial Implications of the Article

The innovation of this study lies not only in analyzing the impact of the social application of facial recognition technology on the protection of personal information rights but also in conducting in-depth explorations of the complex relationship between this technology and individual privacy rights through typical criminal and civil case analyses. The research findings reveal significant challenges in data processing and privacy protection despite the significant contributions of facial recognition technology to social security and services. By combining literature reviews, case studies, and international comparative analyses, this article provides support and recommendations for the practice and policy formulation of personal information protection in the digital age. The article not only assesses the adequacy of the existing legal framework but also explores the impact of technological progress on the protection of facial information rights and the pathways for China to construct effective strategies for facial information protection on the international stage. Additionally, the managerial implications proposed in this study emphasize the necessity of seeking a balance between technological innovation and the protection of personal information.

[40] California Legislative Information. (2018). California Consumer Privacy Act of 2018. Assembly Bill No. 375. Retrieved from https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[41] California Secretary of State. (2020). Proposition 24: California Privacy Rights Act (CPRA). Retrieved from https://www.sos.ca.gov/elections/upcoming-elections/general-election-november-3-2020/proposition-24.

[42] Personal Information Protection Commission (Japan). (2017). Act on the Protection of Personal Information (Revised). Retrieved from https://www.ppc.go.jp/en/legal/.

[43] Ministry of Government Legislation (South Korea). (2011). Personal Information Protection Act. Retrieved from http://www.law.go.kr/lsInfoP.do?lsiSeq=187994&efYd=20111230#0000.

7.2. Differences from Previous Research

Building upon the findings of case analyses and previous research, this paper proposes a series of recommendations to improve the protection of personal information rights. This includes updating existing legal frameworks to adapt to rapid technological advancements, enhancing technological security measures to prevent the misuse of personal data, and increasing public awareness of personal information rights.

7.3. Limitations and Future Directions of Research

The limitations of this study lie in the limited number, scope, breadth, and depth of case analyses, which cannot comprehensively reflect all potential issues and challenges. Future research can expand the scope of case analyses to include more countries and regions, achieve in-depth research on the interaction between technology and law, especially at the international level, and explore the ethical issues of facial recognition technology in different cultural and social contexts. Through more case samples, a thorough investigation of the above issues should be conducted, and attention should also be paid to the dynamic interaction between technology and law, as well as how to promote technological innovation and social progress while protecting personal privacy.

In summary, this paper provides a new perspective for understanding the role of facial recognition technology in modern society and offers theoretical support for the formulation and implementation of relevant policies. It helps guide policymakers in updating laws and policies to address new challenges brought about by technological developments, promotes international cooperation, and collectively enhances the global protection level of facial information rights.

References

[1] Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.
[2] Beijing University Law School. (2021). Research on Face Recognition Technology and Personal Information Protection [J/OL]. Beijing University Law School Official Website. https://www.law.pku.edu.cn/xwzx/xwdt/145004.htm.
[3] Center for Chinese Philosophy Research. (2015). Privacy Theory: Scholar Nissenbaum Proposed the "Contextual Privacy Theory," Emphasizing that the Acquisition and Utilization of Information Should Follow Fair Principles and Not Overly Infringe on Personal Privacy [J/OL]. Center for Chinese Philosophy Research Official Website.
[4] Solove, D. J. (2022, September 8). On the Limitations of Privacy [Lecture]. Peking University Law School "Digital and Rule of Law" Series Forum. Retrieved from Peking University Law School Website https://www.law.pku.edu.cn/xwzx/xwdt/142908.htm.
[5] YouTube. (2022). How to Bake the Perfect Chocolate Chip Cookies. https://www.youtube.com/watch?v=qIiG5VaLnWc.
[6] Friedman, B., & Ferguson, A. G. (2019). Here's a Way Forward on Facial Recognition. The New York Times. Retrieved from The New York Times website.
[7] Bu, Q. X. (2021). The Global Governance on Automated Facial Recognition (AFR): Ethical and Legal Opportunities and Privacy Challenges. International Cybersecurity Law Review, 2.
[8] Fan, Y. R. (2022). Legal Protection Research on Face Recognition Information in the Perspective of Civil Code—Starting from the "First Case of Face Recognition" in Hangzhou [J]. Dispute Resolution, 8(2), 232-237.
[9] Gao, Z. S. (2022). Legal Regulation of Facial Recognition Information Processing Behavior [J]. Learning Forum, (01), 130-136. DOI:10.16133/j.cnki.xxlt.2022.01.017.
[10] Shi, J. Y., & Liu, S. Q. (2021). Protection of Personal Information in Facial Recognition Technology—Discussion on the Construction of Dynamic Consent Model [J]. Financial and Economic Law, 2021(2), 60-78.
[11] National People's Congress. Decision on Strengthening Network Information Protection [DB/OL]. (2020-12-21) [2024-05-03].
[12] Liu, J. P., & Yang, Z. Q. (2021). Privacy Issues Analysis of Facial Recognition Technology and Its Legal Countermeasures [J]. Science and Law (Chinese and English), 2021, (06), 18-28. DOI:10.19685/j.cnki.cn11-2922/n.2021.06.003.
[13] Jin, X. (2023). Making Facial Information More Effectively Protected (People's Comment). People's Daily.
[14] Cheng, X. (2021). Understanding and Application of Personal Information Protection Law. China Legal Publishing House.
[15] Long, W. Q. (2022). Expert Comments on the First Case of Facial Recognition Dispute. People's Court Daily, Top Ten Cases of People's Court in 2021. Retrieved from People's Court Daily Website: https://www.pkulaw.com
[16] Jiang, P. Y., & Du, Y. Y. (2023). Analysis of Privacy Issues of Face Recognition Technology [J]. Yunnan Social Sciences, 2023, (04), 63-69.
[17] Zheng, Z. J., & Huang, Z. X. (2023). Dilemmas and Solutions of Privacy Protection in the Big Data Era [J]. Legal Studies (Hans), 11(4), 3035-3040.
[18] He, N., Chen, Y. J., & Yang, D. R. (2020). Research Status and Hotspot Analysis of Privacy Issues in the Background of Big Data—Statistical and Content Analysis Based on 84 Journal Papers [J]. Frontiers of Social Science, 9(10), 1541-1547.
[19] Civil Code.
[20] Regulation on the Administration of Internet Data Security (Draft for Solicitation of Comments).
[21] (2021) Shanghai 0120 Criminal First Instance No. 828.
[22] Luo, X. (2023). Limits and Application of Criminal Regulation on Facial Recognition—Taking Guiding Cases of Infringement of Citizens' Personal Information Crime as an Entry Point [J]. Comparative Law Research, 2023(2), 17-30.
[23] Opinions of the National Development and Reform Commission, the Central Comprehensive Governance Office, the Ministry of Science and Technology, and other departments on Strengthening the Construction and Networking Application of Public Security Video Monitoring for Public Safety.
[24] Personal Information Protection Law.
[25] (2019) Zhejiang 0111 Civil First Instance No. 6971.

[26] (2020) Zhejiang 01 Civil Final No. 10940.
[27] Xu, M., & Han, S. C. (2021). Prudent Handling and Strict Protection of Biometric Information [J]. People's Justice, (23), 4-8. DOI:10.19684/j.cnki.1002-4603.2021.23.028.
[28] Zhao, J. W. (2020). Attribution and Protection Paths of Face Recognition Information in the Perspective of Civil Code [J]. Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition), 33(5), 21-29.
[29] Cyberspace Administration of China. (August 8, 2023). Provisions on the Security Management of Face Recognition Technology Applications (Trial) (Draft for Solicitation of Comments).
[30] European Parliament and Council of the European Union. (2016). 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). Official Journal of the European Union, L 119, 1-88.
[31] California Legislative Information. (2018). California Consumer Privacy Act of 2018. Assembly Bill No. 375.
[32] California Secretary of State. (2020). Proposition 24: California Privacy Rights Act (CPRA). Retrieved from https://www.sos.ca.gov/elections/upcoming-elections/general-election-november-3-2020/proposition-24.
[33] Personal Information Protection Commission (Japan). (2017). Act on the Protection of Personal Information (Revised).
[34] Ministry of Government Legislation (South Korea). (2011). Personal Information Protection Act. Retrieved from http://www.law.go.kr/lsInfoP.do?lsiSeq=187994&efYd=20111230#0000.