Legal Regulation and Enlightenment of Face Recognition in the Context of Public Health Emergencies in Countries and Regions Other Than China

Wenjie Wang[1,*] Songhua Huang[1] Ziyin Lan[1] Jiao Guan[1] Wenjie Liu[1] Ruijie Wang[1] Honglin Zhu[1] Yuqing Zhang[1]

[1] *College of Humanities, Hubei University of Chinese Medicine, Wuhan, Hubei 430065, China*
[*] *Corresponding author. Email: zyq95@hbtcm.edu.cn*

ABSTRACT
Face recognition technology has been widely used in many scenarios of social life, especially in the current public health emergencies, its enabling utility is more prominent. However, the risks it contains are evident. Countries around the world have accelerated the progress of legislation on the application of face recognition technology, and the legalization of face information protection has become a new trend in information governance around the world. Through the research on the legislative practice of countries in the European Union, North America and the Asia-Pacific region, this paper puts forward some enlightenments suitable for the national conditions of the country, in order to provide a reference for the legal regulation of face recognition technology in China.

Keywords: *Public health emergencies, Countries and regions other than China, Face recognition, Legal regulation.*

1. INTRODUCTION

As the strategic technology and core driving force of a new round of scientific and technological revolution, artificial intelligence provides an important opportunity for intelligent response to public health emergencies [1]. Face recognition technology is a biometric recognition technology based on certain features and digital information of an individual's face [2]. In the fight against the global COVID-19 pandemic, it has released a great empowerment effect in all aspects of the crisis response cycle. However, face recognition technology itself has technical risks. Once abused, it will violate civil rights, endanger social order, and destroy community trust. At present, the existing legal regulation of face recognition technology in China is characterized by decentralization and fragmentation, and the post-event regulation logic of the law itself is even more difficult to effectively regulate the application of technology and prevent the abuse of technology. By sorting out and comparing the legal regulations on face recognition in the European Union, North America and Asia-Pacific countries, and drawing on the experience of foreign legislation, this paper proposes a personal information protection and governance strategy suitable for China's national conditions.

2. LAWS AND REGULATIONS ON FACIAL RECOGNITION IN COUNTRIES AND REGIONS OTHER THAN CHINA

2.1 EU

2.1.1 Commonality

The European Union adopts a comprehensive legislative model, which incorporates all personal information of different types, attributes and levels

into the General Data Protection Regulation (GDPR), integrating administrative, civil and related protection paradigms. The European Union has banned the development of "face recognition" for some time, and at this stage there is a trend of gradually shifting to the direction of prudent use ("Table 1").

Table 1. Key points of EU legislation

Time	Name	Main point
2018	General Data Protection Regulation (GDPR)	There are systematic regulations on the processing of special information such as face recognition. For example, the three principles of "prohibition of processing", "express consent" and "legal necessity" are specified as specific legal principles for the processing of sensitive personal data.
2019	Facial Recognition Technology: Fundamental Rights Considerations in Law Enforcement	Focusing on the implications of fundamental rights involved in the use of facial recognition technology. The focus is on the use of facial recognition technology for law enforcement and border management purposes.
2019	"Guidelines on the Handling of Personal Information via Video Devices" No. 3/2019	This guide can be regarded as a relevant guide for face recognition technology. It involves many restrictive regulations on video surveillance, including that users must clearly inform the monitored object of their monitoring behavior and the date of use.
2021	"Guide to Facial Recognition Technology"	1. Public authorities are prohibited from using face recognition technology in a private environment, except for public safety in a state of emergency. 2. The subject of technology use shall ensure the fairness, transparency and accuracy of the use of face recognition technology. 3. Comply with the principles of purpose limitation, data minimization and storage time.

2.1.2 Personality

Although the General Data Protection Regulation (GDPR) can be directly cited by its member states, due to differences in cultural, economic and legislative values among member states, they have different attitudes towards the regulation of face recognition technology, so they have transformed it into domestic law according to their own national situation and needs. At present, except Greece, Portugal and Slovenia, the remaining 24 member states have incorporated the GDPR legislative rules into their existing legal systems through different forms, and stipulated the powers of their national data protection authorities (DPA) ("Table 2").

Table 2. Key points of legislation of some EU countries

Country	Act	Main point
France	French Data Protection Act	1. The Act applies where the data controller and the data processor are located in France, irrespective of the location of the data processing. 2. Additional expansions have been made on the rights of the data subject, mainly including the ex post management rights of the data subject and the special weekly exclusion right of minors.
Germany	German Federal Data Protection Act	1. On the basis of the GDPR, some additional provisions for the processing of special categories of data (FDPA) have been added. 2. The Act introduced clauses that derogate from the rights of personal data subjects, such as the right of exclusion. 3. This Act sets out criminal offences that may result in imprisonment or fines.
Netherlands	General Data Protection Regulation Enforcement Act (AVG)	1. The Act implemented special regulations applied to personal data relating to automated decision-making, journalism and art. 2. While strengthening the supervision of the consumer market, it has clarified its main responsibility as an economic activity.

Country	Act	Main point
Spain	Organic Law 3/2018 of December 5 on the Protection of Personal Data and the Granting of Digital Copyrights ("Spanish Data Protection Law").	1. Organizations should retain data for a period of time in order to assert legal rights before data deletion. 2. This law has improved the processing and storage of criminal data. Unless it is necessary for clear and legitimate purposes, only the consent of the data subject cannot be used as an exemption clause for data processing.
Italy	"Act" No.108 of 2018	1. The safeguards for genetic data, biometric data and health data are required to be updated every two years. 2. Criminal penalties will be imposed on anyone who fraudulently obtains automatically generated files or substantial portions thereof that have been processed on a large scale and contain personal data for profit or to cause harm to others.

2.2 North America

2.2.1 United States

2.2.1.1 Federal Level

The United States does not have a unified legal regulation on the collection and use of face recognition data at the federal level, and its legal regulation varies with different subjects and purposes. Generally speaking, it is a prudent and hierarchical strict attitude [3]. This decentralized legislation regulates the processing of biometric information with a special bill, which can clarify the information subjects of specific types of information and the legal relationship between information collection and utilization subjects, solve problems more targetedly, and make standardized application of face recognition more practical. ("Table 3")

Table 3. Legislation at the federal level

Time	Name	Main point
2019	Business Facial Recognition Privacy Act	1. This Act regulates the application of face recognition technology in the business field. Commercial companies are prohibited from sharing their photo data without the express consent of the photo owner. 2. It is required that business entities related to face recognition must obtain personal consent when using face recognition technology.
2019	Facial Recognition Technology Authorization Act	It aims to limit the use of facial recognition technology by agencies such as the FBI's Immigration and Customs Enforcement, making it clear that facial recognition technology can only be used for continuous surveillance under circumstances such as a court order.
2019	Facial Recognition Assurance Act	1. The Act forces law enforcement agencies to use face recognition technology for surveillance, an arrest warrant shall be obtained based on the content of the suspected crime, and exemptions may be considered in special circumstances; 2. About the use of face recognition technology in the field of law enforcement, the approval period is a maximum of 30 days and should be obtained to a minimum. 3. The Act supervises the judge's decision-making power and requires the judge to report the approval result of each request to the US Court Administrative Office.
2020	Ethical Use of Facial Recognition Act	1. The Act requires to establish a congressional committee to develop guidelines for the use of facial recognition technology in the United States. 2. Before the committee issues guidelines for the use of facial recognition technology, the use of facial recognition technology by government agencies needs to be limited.

Time	Name	Main point
2020	National Biometric Information Privacy Act	1. This Act applies to "private entities". This generally includes businesses of any size that possess any individual's biometric identifier or biometric information. 2. This Act requires the individual's consent before the collection and disclosure of personal biometric identifiers and information. 3. Private right of action against entities protected by the Act, gives the aggrieved individual the right to recovery. 4. There is an obligation to protect biometric identifiers or biometric information in a manner similar to how organizations protect other confidential and sensitive information, such as social security numbers.

2.2.1.2 State and City Level

Some states and cities in the United States have made special legislation on face recognition based on their own development. The legislative orientation and regulation are different. At present, eight states or cities have already introduced relevant laws. States and cities that have legislated are more concerned about the government's use of facial recognition technology in public places, arguing that people's freedom and privacy have been violated. It should be noted that although some states in the United States have a more lenient legislative attitude towards the public management and use of biometric information, but it does not affect the legislation of some cities to explicitly prohibit the use of face recognition technology. ("Table 4")

Table 4. Some state and municipal legislation

State and city name	Time	Name	Main point
Illinois	2008	Biometric Privacy Act	It is the first law in the United States to protect personal biometric information. It is stipulated that entities collecting facial information must notify the person being collected or their legally authorized representative in writing, distinguishing the traditional principle of consent into written notification and written authorization.
California City of San Francisco	2019	"Regulations on Stopping Secret Surveillance"	It completely prohibits local government departments from using face recognition technology, and regards the direct use of face recognition and the acquisition of certain information through technology as illegal acts. It is the first city in the world to introduce a ban on face recognition.
Washington State	2020	Facial Recognition Service Act	1. State or local government agencies need to submit accountability reports to the legislature when developing, using, or acquiring facial recognition services. 2. Legal, independent and reasonable tests on the face recognition service must be conducted in an operational state to ensure accuracy. 3. Technicians engaged in facial recognition services require regular training.
California	2020	Face Recognition Technology Law	1. This Law grants individuals the right to confirm, delete, withdraw, and correct or challenge facial recognition information. 2. Injunctive penalties are provided, with civil penalties not exceeding $2,500 for violations or $7,500 for willful violations.

State and city name	Time	Name	Main point
Texas	1952	Uniform Commercial Code (2021 revision)	The biometric information of the information subject shall not be obtained without obtaining consent. Unless certain conditions are met, biometric information cannot be sold or disclosed to other parties.
Massachusetts Somerville	2019	"Regulations on Prohibiting the Facial Technology Surveillance"	The second city in the United States to ban the use of facial recognition technology by public authorities, but not to restrict the use of facial recognition technology by state governments or federal law enforcement.

2.2.2 Canada

In Canada, facial recognition technology is already being used in some police departments. Canadian laws regulating personal information mainly include the federal government's "Privacy Act" and the "Personal Information Protection and Electronic Documents Act" (PIPEDA) that regulates corporate behavior. There is no specific mention of characteristic data such as facial recognition, and it is in a less regulated position. It is worth noting that in recent years, cases such as the "Vancouver Child Sexual Exploitation Case, the police illegal use of facial recognition software" and the "Illegal Collection of Facial Information by Canadian Shopping Center Operators" have brought the issue of face recognition legal regulation to the forefront, and everyone called for the reform of the personal information law framework. In November 2020, based on the general trend of the reform of the personal information law framework and the problem of improper use and leakage of personal information in the prevention and control of the COVID-19 pandemic, Canada issued the "Digital Charter Implementation Act 2020" (C-11 Act) to tighten regulation of businesses that handle private, sensitive information Divided into the "Consumer Privacy Protection Act" (CPPA) and the "Personal Information and Data Protection Tribunal Act" (PIDPTA), C-11 Act provides the toughest corporate financial penalties in history, private rights of action for individuals, and new rights for individuals (right to data portability and right to erasure). Facial recognition information is a typical representative of sensitive information, and C-11 Act provides it with comprehensive judicial protection.

2.3 Asian-Pacific Region

2.3.1 South Korea

In January 2020, the South Korean National Assembly passed the "Personal Information Protection Act", the "Credit Information Act", and the "Information and Communication Network Act (Amendment)". The "Personal Information Protection Act" (PIPA) includes detailed procedures and methods from formulating national policies for personal information protection to personal information processing and protection. Article 15 of the Act stipulates that personal information processors may collect personal information under specific circumstances and use it within the scope of the purpose for which it was collected [4]. In the context of the COVID-19 pandemic, in February 2020, the South Korean National Assembly revised the "Infectious Disease Prevention and Management Act" (IDCPA), "Quarantine Law" and "Medical Law". These laws, known as the "three new crown laws", have played a key role in South Korea's use of big data to prevent the pandemic.

On June 16, 2021, the European Commission launched the adequacy determination procedure for the transfer of personal data in South Korea. The Committee assessed the legal and practical level of personal data protection in Korea, including the rules for providing personal data to government agencies, and concluded that its legislation has substantially the same level of protection as the General Data Protection Regulation.

2.3.2 Japan

Japan enacted the "Amendment to the Personal Information Protection Law" in 2020. In September 2021, the Personal Information Protection Commission (PPC) of Japan announced an update to the Q&A on the guidelines on the "Act on the

Protection of Personal Information", adding relevant specific provisions on use of facial recognition information, personal data breach reporting, pseudonymization processing information and personal reference information, cross-border transfer of personal data, etc.; this update focuses on the use of face recognition information. Data processors need to abide by the revised "Act on the Protection of Personal Information" when collecting face recognition information, and make corresponding regulations on the application of face recognition in public places to prevent or defuse the potential risks of personal information protection in the era of big data.

Japan has enacted the "Administrative Organs Personal Information Protection Act", the "Independent Administrative Agency Personal Information Protection Act", and the "Personal Information Protection Regulations" for local public organizations. The main purpose is to protect national administrative agencies, local public organizations, independent administrative agencies and other public authorities to regulate respectively. Based on the needs of COVID-19 pandemic prevention and control, these specific legislation can better balance the game between "personal priority" and "public priority": starting from personal priority, specific personal information (sensitive information) needs to be considered; starting from public priority, general personal information is based on the principle of restricting misuse [5].

2.3.3 Singapore

Currently, Singapore mainly restricts and regulates the collection, use, disclosure and processing of personal data by organisations through the "Personal Data Protection Act" (PDPA) in 2012. In its nine data processing principles, the law clarifies that when organizations collect, use or disclose facial recognition information, they need to obtain individual consent and undertake the obligation to inform the purpose of use, and allow individuals to withdraw consent. Individuals also have the right to request that institutions provide access to and correct facial recognition information. At the same time, the law limits the retention period and transfer commitment of facial recognition information. The accompanying "Personal Data Protection Regulations" have focused on regulating the access, correction and transfer of personal data such as face recognition information.

The "Personal Data Protection Act" was revised in 2020. The revised draft has strengthened institutional accountability, added relevant content such as the right to portability of personal data and data transmission obligations, and increased the amount of fines. The cost of violations has increased. Despite the increased penalties, the new regulations also provide more space for companies to use facial information. Organizations may collect, use or disclose personal data without obtaining consent from individuals as long as it is in their "legitimate interests" or for public interest purposes, such as preventing fraud and improving products. However, a risk and impact assessment must be carried out first.

3. IMPLICATIONS FOR CHINA

From the perspective of comparative law, the United States and the European Union represent two different paths: The EU as a whole strictly restricts the use of biometric information, but at the same time gives EU member states certain discretionary powers, allowing member states to stipulate that restrictions on biometric information do not apply under certain circumstances; The United States does not restrict the use of facial recognition data at the federal level, giving states and spheres great regulatory authority. Countries and regions such as the United States and the European Union have accumulated rich experience in legislation and protection, which has important reference significance for the legal regulation of face recognition technology in China.

3.1 Establishing a Risk Assessment and Prediction Mechanism

Against the background of the era of big data, the global response to public health emergencies has accelerated the widespread application of face recognition technology, but face information recognition embedded in personal biometric tags also faces great legal risks, such as error risks, risks of identity authentication being cracked, risks of information leakage, etc. Once 100% identifiable biometric information is leaked or used improperly, the consequences are incalculable, accompanied by serious public safety problems, and even more crimes to some extent. . Therefore, laws and regulations for the application of new technologies should adopt a relatively flexible and open legislative model, leaving room for legal operations when preventing and controlling risks [6].

Europe and the United States have adopted differentiated governance solutions for the two types of users, government agencies and commercial agencies, that is, they adhere to the principle of strong risk prevention when using face recognition technology in public places and government agencies, and follow the principle of weak risk prevention in commercial applications. China should also actively establish a risk assessment and prediction mechanism, namely: (1) Before collecting and using personal information, first conduct a risk assessment, which can be learned from the practice of establishing a "Facial Recognition Working Group" in Washington State's "Facial Recognition Service Act", to review the potential risks, legal adequacy, rights infringement and other issues of face recognition technology. (2) According to the evaluation results, it can be divided into weak risk and strong risk situations; (3) Different response measures are formulated for different risks. In the case of weak risk, the government is required to analyze and measure the costs and benefits. In the case of strong risk, the government is required to take preventive measures even if there is no scientific evidence, so as to avoid the consequences of greater damage as much as possible.

3.2 Improving the Regulatory Framework for the Application of Face Recognition Technology

Based on the complexity of face recognition technology and its deficiencies in technical specifications and legal regulations, there is a risk of being abused. It is particularly important and necessary to improve the regulatory framework for the application of face recognition technology, which mainly includes the following:

3.2.1 Clarifying the Supervisory Authority and Supervisory Responsibilities

It is necessary to further clarify the regulatory agencies and regulatory responsibilities at the central and local levels, highlight the leading role of the national and local network information offices, and avoid the ambiguity and randomness of multi-level supervision.

3.2.2 Improving Access Mechanism to a Strict Level

China can refer to the manual review and testing mechanism of Washington State, the United States, to improve the entry threshold of the industry, and the national network information department can conduct a systematic assessment of enterprises in terms of business scope, technology application methods and fields, face information storage security, and algorithm non-discrimination. Collectors, controllers and processors of biological information can only engage in activities related to the collection, storage and processing of personal biological information after they have been approved and obtained the application license [7].

3.2.3 Setting up a Third-party Supervisory Agency

China can refer to the "Biometric Information Privacy Investigation Commission" of the State of Illinois to set up a third-party regulator. This institution is an important subject to prevent technology abuse and ensure information security. The supervisory agency implements dynamic supervision, strengthens the supervision before and during the event, and realizes the supervision of data security through principled reviews such as necessity and rationality, as well as specific industry evaluation standards. China can also refer to the data protection personnel mechanism in the EU rules, and select professionally qualified personnel to regularly send on-site supervision to major face recognition technology businesses.

3.2.4 Guaranteeing Informed Consent Effectively

In the process of technology application, high notification standards should be set for processing face information, so that autonomy of will can fully penetrate into individual decision-making and truly implement "autonomous control". Users' informed consent and detailed rights management should also be implemented simultaneously. The relevant provisions of Singapore's PDPA can be refered to give users the right to withdraw consent. After the withdrawal of consent, organizations must stop collecting, using or disclosing these personal data.

3.2.5 Strengthening Supervision

It is necessary to continuously standardize the supervision procedures, improve the accountability system, clarify the punishment measures, and establish a complete supervision and evaluation mechanism for the application of face recognition technology.("Figure 1")

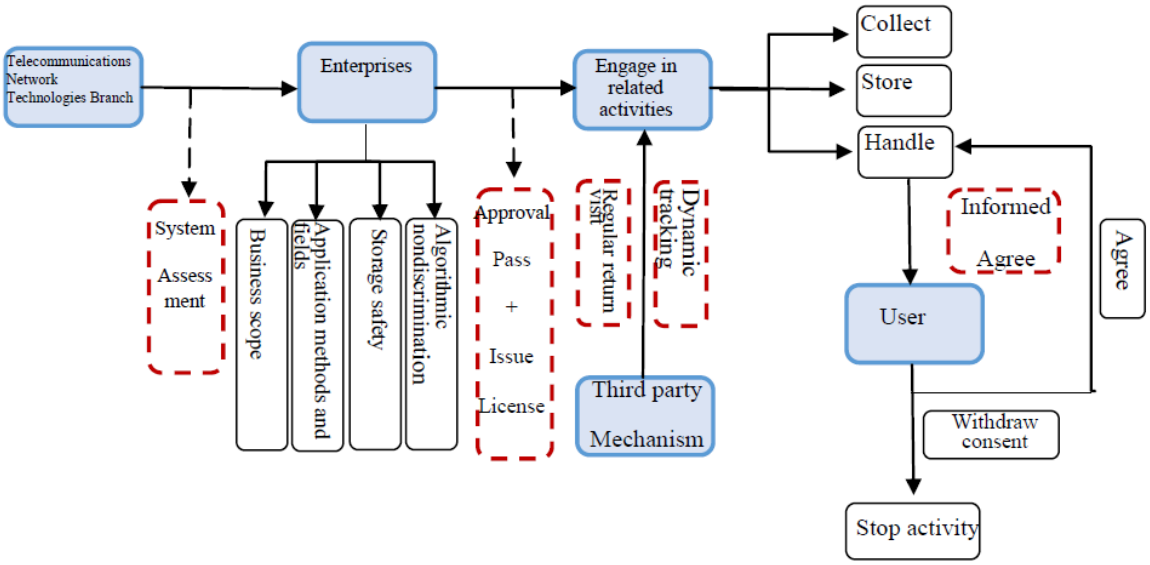

Figure 1 Regulatory framework for the application of face recognition technology.

3.3 Regulating Industry Self-discipline

The United States pursues more pragmatism in personal information protection, values the benefits brought by information circulation, and delegates power to mature industry associations and organizations on the basis of government guidance [8]. Canada chose the "middle way". The promulgation of the "2020 Digital Charter Implementation Law" requires the industry to self-discipline, and uses severe punishment measures to ensure the effective operation of information protection within the industry. In the context of public health emergencies, it is necessary to stimulate the endogenous power of information protection in the industry at the national level, and at the same time use coercive law to ensure its healthy operation and promote the formation of industry self-discipline. Face recognition-related industries should also establish self-discipline and internal mechanisms, such as enhanced tracking, access control, data encryption and other mechanisms to ensure data security, and strive to implement the concept of balancing personal information protection and business development.

3.4 Improving Post-mortem Relief Methods

Facial information has the unique characteristics of being specific and difficult to change. If it is illegally violated by leakage or theft, it may cause irreversible and permanent damage to the information subject. As in public health emergencies, it is mainly the administrative agencies or their entrusted agencies that collect and use facial information for public interests. Therefore, under the protection mechanism of administrative laws, China can learn from the EU GDPR or the systems of Asian and European countries to establish the right of administrative complaint, to safeguard the legitimate rights and interests of citizens through administrative litigation; under the civil legal protection mechanism, China can refer to the practice of BIPA in Illinois, the United States, to clarify the dual rights relief methods of "spiritual and economic compensation" in legislation, formulate damage determination standards, and add public interest litigation relief methods. At the same time, the minimum or maximum compensation amount can also be set by referring to the practice of BIPA and GDPR. If the actual loss is lower than the minimum compensation amount, the victim can also file a claim with the minimum compensation amount; under the protection mechanism of criminal law, it may be considered to set up such as the crime of "illegal handling of unique identifiers" in South Korea and the crime of "theft of personal identification methods" in the United States and other crimes to improve the bottom line protection of personal biometric information.

4. CONCLUSION

Humans cannot overcome major disasters and epidemics without scientific development and technological innovation [9]. As a representative technology of the new generation of information

technology, face recognition can provide technical support for the management of public health emergencies. At the same time, since the personal information corresponding to face recognition technology covers multiple legal interests, if there is no scientific and effective legal regulation, it will inevitably induce complex and diverse social risks. Therefore, a one-size-fits-all model of prohibiting use does not conform to my country's national conditions. "Promoting a responsible use" and taking the development needs of national conditions as the legislative limit are the direction of legal regulation of technology application in China.

AUTHORS' CONTRIBUTIONS

Yuqing Zhang contributed the central ideas and was responsible for the final revision of the paper. Wenjie Wang designed the thesis outline, coordinated the writing arrangement of the paper, and revised the first draft. Songhua Huang, Ziyin Lan and Jiao Guan revised the thesis outline, collected and analyzed data. Wenjie Liu, Ruijie Wang and Honglin Zhu collected and analyzed typical cases. All authors analysed the literature and were involved in writing the manuscript.

REFERENCES

[1] Wang Huiquan, Liu Lu, Governance of Public Health Emergencies in the Application of Artificial Intelligence [J]. Medicine and Society, 2021,34(07):42-46. DOI:10.13723/j.yxysh.2021.07.009. (in Chinese)

[2] Li Qingfeng, Legal Regulation of Face Recognition Technology: Value, Subject and Grasp [J]. People's Tribune, 2020(11): 108-109. (in Chinese)

[3] Xing Huiqiang, Legal Regulation of Face Recognition [J]. Journal of Comparative Law, 2020(5): 51-63. (in Chinese)

[4] Ma Guang, The Protection of Personal Information in Epidemic Prevention and Control [J]. Science Technology and Law, 2021(04): 29-36. (in Chinese)

[5] Zhang Hong, Research on Japanese Act on the Protection of Personal Information in the Era of Big Data [J]. Law and Economy, 2020(03): 150-160. (in Chinese)

[6] Zhang Yong, Legal Protection of Personal Biometric Information Security — Take Face Recognition as an Example [J]. Social Sciences Digest, 2021(08): 8-10. (in Chinese)

[7] Luo Pan, Legal Regulation of Personal Biometric Information Processing in Face Recognition [C]//"Shanghai Legal Research" Collection (Volume 5, Vol. 53 in 2021) - Proceedings of the 2021 World Artificial Intelligence Conference Rule of Law Forum, 2021:109-117. (in Chinese)

[8] Li Chunqin, Jin Huiming, On the Enlightenment of Personal Information Protection in the United States to China — From the Perspective of Industry Self-discipline [J]. Business China, 2010(02): 303. (in Chinese)

[9] Xi Jinping, General Secretary Xi Jinping's Important Speech at the Symposium of Experts and Scholars Pointed out the Direction of Scientific Research [EB/OL]. http://www.xin-huanet.com/politics/leaders/2020-06/04/c_1126074999.htm. (in Chinese)