DOI: 10.37420/j.mlr.2023.012

Exploration of Administrative law regulation path of facial recognition technology infringement: New challenges, new contradictions, new countermeasures

Pucheng You
The Law School of Beijing Normal University, Beijing, China
***Corresponding author, E-mail: youpucheng 2021@126.com**

Abstract
In recent years, facial recognition technology has been widely used in military, security, finance, government and other fields. It has greatly improved the efficiency of market operation and social management, but at the same time, it has also initiated various legal disputes. Telecommunications network fraud, illegal issuance and collection of loans and many other network information security problems remain high, which should be paid special attention and taken great care. In order to balance legal conflicts and contradictions between personal interests and public interests, promote the harmony and stability of the legal order, and enhance judicial satisfaction of enterprises and the masses, this paper intends to combine the legal provisions of administrative law and relevant judicial interpretations, review the new challenges brought by facial recognition technology as well as the new problems existing in administrative law regulation, and thus put forward the regulatory paths for the application of facial recognition technology under the perspective of administrative law.

Keywords
Facial recognition technology; Facial information; Administrative Legal System; Digital governance; Regulatory paths

Introduction

Facial recognition technology, commonly known as “face swiping”, is a kind of biometric identification technology based on people’s biometric information for identity authentication. It is composed of a series of discrete sub-processes such as facial image collection, facial image preprocessing, feature extraction and comparison recognition. At present, China has entered the era of large-scale release of digital economy dividends, the scope of application for human-machine coexistence and human-machine interaction continues to expand, thus inevitably producing significant risks of excessive collection and illegal use of personal information.

The research on the legal regulation of facial recognition technology has always been one of the hot spots in the academic circle. The reason why this paper chooses to study it under the perspective of administrative law includes the following two necessities: (1) At the academic level, when discussing the regulation of facial

recognition technology, the current academic circle rarely has a binary scenario that distinguishes between public and commercial use, and often confuses it when discussing it in detail. To be exact, nowadays, most research directly focuses regulation field on the commercial use and completely ignores the situation that the administrative department of the government as the main body collects and processes facial information for the purpose of public management; (2) At the practical level, government administrative departments mostly use facial recognition technology to assist in completing administrative tasks, and the application field covers administrative licensing, administrative punishment and supervision of new business formats and industries, etc. The fixed and lagging nature of the law determines that if regulatory measures are not taken in time, it is often unable to fully and accurately adapt to complicated social relations. Therefore, while expanding the area of application of facial recognition technology to improve convenience and security of people's lives, it should also be placed under the perspective of privacy protection for reflection and review. Based on this, this paper firstly focuses on the infringement forms of facial recognition technology, and then systematically explains multiple dilemmas confronted by administrative law in regulating the application of facial recognition technology, and finally explores the risk prevention and responsibility of facial information collection and utilization from the perspective of administrative law.

1.New challenges: infringement forms of face recognition technology

Over the years, with the rapid development of networking and computing technologies, facial recognition technology has not only enhanced the people's sense of intelligent service experience, improved the level of social governance, and achieved huge economic benefits, but has exposed unprecedented social and economic crisis. The root cause is that data, as an emerging factor of production, has given facial recognition information multiple attributes of personality, property and national sovereignty, resulting in the dilemma that its right attributes are difficult to type.

First, it causes the violation of personal privacy and security. As the end of all identifiable information, the face is attached to a series of tag attributes that accompany personal identity. These information directly or indirectly carry and express their rights and obligations, and even their personality characteristics and behavior habits. In real life, a host of units often use convenience as a pretext for deliberately accessing all the information about customers through facial recognition. These organizations, however, do not clearly inform information subjects of how the personal information would be processed and what remedies would be taken for the mishandling of information. The general vagueness of the consent mode seriously violates the principle of equality between user agreements.

Second, it undermines the dignity of human personality. Facial recognition technology is essentially an artificial intelligence algorithm, and the algorithm contains massive subjective factors such as subjective initiative and values of the developers. Therefore, it is inevitably accompanied by human biases in the algorithm. Algorithmic black box, algorithmic discrimination and illegal supervision are the most direct and acute challenges to human dignity. With the expansion of information attributes beyond the political scope, the possibility of personal biological information stored in it being leaked, stolen, and abused has increased dramatically, and it can even be associated with personal information in different databases, which is easily reduced to a tool to improve the accuracy and timeliness of facial recognition technology, and even become the object of exploitation and enslaved by a small number of commercial institutions and government departments. For example, some enterprises take photos of customers' faces in order to accurately grasp their tastes, preferences

and consumption patterns, classify them into different categories, and improve successful order rate, which undoubtedly poses severe threat to fair trading rights and personal dignity of customers. What's more, to obtain more interest space, some businesses tend to pay to exchange and share face information database collected by other businesses providing different services. This definitely means that illegal information integration leads to a more in-depth analysis of the individual's information, and intensifies digital personalization and information transparency.

Third, it impairs personal or property rights and interests. Due to the close natural connection between economy and data, facial recognition technology is widely used in economic activities of all walks of life, so personal biometric information identified by facial recognition technology carries a substantial amount of civil rights and interests of the relevant digital subjects. Once the information is being abused, its dual attributes of property interests and personality interests are often more likely to cause irreversible damage to individuals, and these damages are difficult to remedy and may even be permanent. In addition, facial recognition technology has transformed the previous monitoring mode based on manual into an algorithmic monitoring mode, and once the face information is leaked and improperly used, it is indubitably easy to cause major security risks for the information subjects to hold accounts.

2.New contradiction: the dilemma of administrative law protection in the application of facial recognition technology

The application of facial recognition technology has been upgraded from identity recognition to user portrait and real-time tracking, which has led to the continuous expansion of the means of personal information disclosure to a certain extent, and has brought new problems to the protection of personal information. Currently, the protection of face information in our country is principally reflected in the regulation of personal information, and the regulation of personal information primarily adopts the combination of special legislation and decentralized legislation. Considering the particularity of facial recognition, nevertheless, the interpretation and application of law are confronted with a series of tricky problems, for instance, the ambiguity of the rights and interests infringed by facial recognition, the difficulty in identifying harmful behaviors, and the uncertainty of the risk damage. In the following, this paper will discuss the dilemma of administrative law regulating facial recognition technology based on the legislative and judicial levels.

(1) The positioning of personal information rights and interests is unclear, and the scope of information protection is not clearly defined

The Personal Information Protection Law adopts general legislation and "enumeration and disclosure clause", which ensures stability, simplicity and other advantages to a certain extent, and provides a more comprehensive, multi-level and diversified basis for the protection of personal information. For example, Chapter 4 of the Personal Information Protection Law stipulates a great deal of rights enjoyed by individuals in the processing of personal information, like the right to know and decide on personal information, and the right to restrict or refuse the processing of personal information by others. At this stage, however, there are still numerous problems in the connection among the Personal Information Protection Law, the Civil Code, the Criminal Law and other legal provisions, and there are many shortcomings in the operability, which requires

the legislative department to make a complete explanation on their mutual coordination and application. Compared with the legislative model of "basic law summary + supporting regulations (interpretation) listing" and "general + exception" adopted by Japan in the series of laws and regulations on personal information protection, some provisions of the Personal Information Protection Law lack uniform standards for the identification of acts, and the improper and illegal acts of handling personal information are not covered in all aspects, so as to provide operational space for personal information processors to engage in illegal operations. Further, the relevant administrative legislation is not well-targeted and effective, and cannot be fully applied to specific application scenarios. In addition, when individuals collect and use information, they do not adopt the consultation method of "individual consent", and the subsequent processing steps such as the use, processing and transmission of information are often out of personal control, which is peculiarly prone to become a tool for some managers to illegally accumulate wealth.

The high-speed flow of data information is also one of the incentives for the frequent occurrence of personal information leakage. From the point of view of pre-practice norms, data sharing makes the reuse of personal information resources simpler and more direct, and also gives space for those who hold some illegal purposes to engage in illegal activities. Moreover, the disclosure of personal information has high benefits but low costs, which is completely easy to cause secondary crimes. From the perspective of acting in the matter, as the relevant collector with an advantageous position, they are inclined to forget to implement the principle of informed consent and completely ignore the true meaning of the two sides when collecting face recognition information. In real life, a great quantity of information collection parties force users to passively provide facial information by default or offering services for them in the traditional way of exchange, without providing information subjects with more diversified, more flexible and richer choices in accordance with the procedures stipulated by relevant laws, not to mention fully guaranteeing the right of self-determination of information subjects. From the perspective of post-processing, even if the abuse of personal information is detected, the criminal penalty is relatively light, making it difficult to deter the perpetrators.

(2) The main body of administrative supervision is not accurate enough, and the administrative supervision mechanism is not sound enough

Generally speaking, China's current administrative supervision system is a relatively systematic system that suits China's national conditions, with multiple administrative supervision subjects and organizations, and various administrative supervision methods and channels. However, in the concrete supervision practice, the supervisory bodies actually lack effective communication, coordination and cooperation. Specifically, there is no special administrative regulatory body responsible for digital applications such as facial recognition technology in our country. The sixth chapter of the Personal Information Protection Law stipulates that the regulatory system is coordinated by the national network and information technology department, with mixed and decentralized supervision by multiple institutions. That is, the public security organs, the national network information department, the market supervision administration and other state agencies are jointly and severally liable for the regulation. This leads to in the process of administrative supervision, the docking work between various departments is not smooth, and there is a "kicking the can down the road" phenomenon of vague regulatory responsibilities, multiple law enforcement, weak supervision, mutual prevarication, and low efficiency.

The fundamental reason for the overlapping functions and rights of administrative organs is that China's ad-

ministrative laws and regulations have significant characteristics of departmental legislation, and there are a flock of chronic diseases of entrusted legislation and industry legislation. Many administrative laws and regulations only focus on their own departmental interests and industry protection, completely ignoring the overall awareness and systematic concept of laws and regulations. Furthermore, the time of legislation and amendment of various departments of law is inconsistent, the legislative process is often hasty, resulting in the lack of systematic overall consideration and necessary conditions to build an precise and effective administrative supervision system. Also, there is a shortage of practical operational norms and supervision system provisions for facial recognition technology evaluation, supervision, tracking, and specific administrative penalties. Although the law at this stage focuses on the post-normative adjustment of the risk of the application of facial recognition technology, in the end, whether in the prior mechanism, supervision, or in the post-accountability link, the systematicity and pertinency of face information protection in our country are far from enough. When the administrative supervisory personnel exercise the right of supervision, they can only find applicable administrative regulations from the laws and regulations and other normative documents scattered in the Civil Code, Criminal Law, Personal Information Protection Law, Information Security Technology Personal Information security Code. However, such complexity is also more difficult for administrative supervisors, not to mention the serious inefficiency and the effective play of supervision.

(3) The administrative damage compensation mechanism needs to be urgently established, and the administrative litigation relief channels need to be improved

Among the elements of infringement in the application of facial recognition technology, there are huge theoretical disputes over the subject of infringement, the principle of liability, the determination of damage and the cause and effect, which increases the difficulty of relief in judicial practice. Whether to take the right to privacy relief, or choose remedies for personal information rights and interests, it mainly relies on property damage compensation, and is difficult to truly safeguard the rights and interests of the information subjects, not to mention cracking down on information collectors who arbitrarily infringe on face information. In the existing judicial interpretation of mental damage compensation, if the degree of mental pain only reaches the non-serious degree of "general", the victims' mental damage compensation is often difficult to get the support of the people's court.

In legal practice, facial recognition information, with its low cost of infringement and high cost of rights protection, is increasingly showing a trend of being widely collected. However, the intervention of administrative power on illegal activities such as illegal collection, sale and use is too delayed, and corresponding relief measures are often taken after facial recognition information is infringed. There are few sound legal and regulatory systems and institutional guarantee systems in advance and in the process. In addition, the current facial recognition cases are rarely solved through administrative channels, and even if solved through administrative channels, administrative organs are difficult to provide perfect and smooth judicial relief channels.

3 New countermeasures: facial recognition technology application of administrative law regulation path

At this stage, China's administrative law regulation on the infringement of facial recognition technology is

not perfect, the regulatory basis is fragmented and lacks specific directionality, privacy and personal information protection, the public's right to know and information disclosure, data control asymmetry is increasingly significant. With the focus on prior risk control, the research on the application of facial recognition technology in the field of administrative law regulation is relatively scarce. Therefore, while expanding the scope of application of facial recognition technology to improve the convenience and security of people's lives, it needs to be reflected and examined under the perspective of privacy protection. To achieve the balance between the application of facial recognition technology and privacy protection is the top priority of administrative law regulation. Based on the perspective of administrative legislation and administrative supervision, this paper puts forward three methods to make up for the limitations of criminal and civil application regulation of facial recognition technology.

(1) Establish the pre-administrative prevention mechanism that refine government responsibilities and raise technical standards

Clarify the meaning of legal norms on information protection and the specific functions and powers of the government. First, specify the legal concepts involved in the Personal Information Protection Law. For example, there are uncertain concepts such as "minimum scope" and "public interest" in the legal provisions on the collection links, which tend to make the illegal infringement of the collection subjects out of legal control. Second, according to the different application scenarios and application needs of face information, the administrative organs and authorized state-owned enterprises and institutions have the powers of licensing, review, supervision, punishment and other administrative acts on the application of facial recognition technology. Third, define the boundaries and principles of collecting and processing face information by administrative organs when applying facial recognition technology, and strictly divide the scope of application into three categories: should be used, can be used and do not need to be used, so that the information collection subjects can minimize the adverse impact of natural persons when using face information. Relevant departments must also strictly abide by the provisions of the Personal Information Protection Law necessary for the purpose of maintaining public safety, and may not collect and process face information for other illegal and non-compliant purposes. Fourth, raise the industry's access threshold of non-governmental organizations from the source, and introduce a multi-level and diversified administrative licensing system for facial recognition technology. The face information control subjects must obtain the qualification certificate issued by the relevant state departments before it engages in the collection, storage, processing and other activities of face information.

Strengthen the government's responsibility to protect citizens' face information. In view of the objective effectiveness and necessity of face information in the management of public affairs, government departments have created citizens' legal identity information, and should assume the responsibility of protecting citizens' face information, while taking multiple measures to enhance citizens' awareness of protecting legitimate rights and interests of face information. On the one hand, the government departments need to give the basic rights of the facial recognition information subject, such as by holding lectures on network information technology law popularization, printing and issuing brochures to prevent personal information infringement, etc., clearly informing citizens of the rights and obligations associated with face information and the legal basis for collecting and processing information. On the other hand, government departments should also further clarify the obligation to inform, guarantee security obligations and legal processing obligations of facial recognition technology application subjects in the process of collecting and using face information, and order organiza-

tions to promptly inform information subjects of collection reasons, storage periods, storage security, remedy approaches and other specific contents of the collection and use of facial information. Only in these methods can citizens' information rights, independent choice rights, fair trading rights, rectification rights, expurgation rights be fully protected. In a word, the government needs to pay special attention to the coordination and balance of public interests and personal interests in public places, neither to seriously harm personal interests due to excessive maintenance of public interests, nor to hinder the development of biometric identification industry due to the inviolability of personal information rights.

Formulate specific standards and requirements for facial recognition technology. From the perspective of technology optimization, government departments should constantly promote the improvement of legal identity information technology, reduce the shortcomings and deficiencies of facial recognition technology in equipment and facilities and operation, so as to curb the manipulation of facial recognition technology by counterfeiting, stealing, cloning and other violations of laws and regulations and human ethics, reduce social crimes, and maintain social order and stability. From the perspective of system design, government departments should constantly improve the facial information regulation content in various departmental laws, formulate specific security management systems for the collection and use of personal information in the field of public administration and market economy and related activities, accelerate the development of technical standards system and legal protection system for facial recognition applications, and coordinate the rights and obligations of private interest subjects in different legal norms. For example, application subjects, application scenario, application depth and breadth of facial recognition technology should be specified in different categories, especially the focus of comprehensive harness should be placed on the access rights and ways of facial information in different application scenarios.

(2) Establish an in-process administrative supervision mechanism for administrative accountability supervision

Build a whole-process government supervision and management model. Based on the long-term and complex risks of facial recognition technology, government departments should fulfill the obligation to guide citizens to pay close attention to the use of face information, and establish a "fully integrated, all-round and whole-process" administrative law enforcement coordination and supervision system with high standing and high standards, which can not only effectively supervise the government's performance of functions, but guarantee citizens' rights and interests with high quality. To be specific, the government needs to confirm the first time whether the collection and use of facial information is due to the true intention of citizens, and inform the use of citizen identity information in a timely manner, so as to avoid others using the time interval to steal or obtain personal information by other illegal methods. If the information leakage is further expanded, the government departments can also accurately crack down on illegal and criminal activities that use and falsify citizens' facial information, timely sanction offenders who use citizenship information, and determine the important basis for their future legal consequences.

Set up a special administrative accountability supervision body. In the digital society, the granularity of information such as human body, social relations, political and economic data is further refined, and is obtained, analyzed and evaluated in a more precise and thorough way. In recent years, although China has successively established national regulatory agencies such as "Cyberspace Administration" and "State Information Center" as well as provincial and municipal regulatory agencies such as "Big Data Application Development Admin-

istration", it is undeniable that the regulatory model, scope and standards of multiple administrative departments lack a certain systematics. In fact, the relationship between the powers and responsibilities of these regulatory bodies has extremely serious crossover, ambiguity and blank areas. It not only greatly reduces the efficiency of government work and seriously damages the credibility of the government, but gives criminals a great many opportunities to use personal information to engage in illegal and criminal activities, hindering the construction of a promising and responsible government. Therefore, it is exceedingly necessary to define the subject of administrative supervision in the form of law and establish a personal information regulatory body specifically responsible for identifying, evaluating and controlling personal information, so as to effectively make up for the absence of regulatory subjects and improve administrative efficiency and social governance. The specific functions of these institutions should include: carrying out differentiated, classified and graded supervision on developers and processors of facial recognition technology, timely making preventive warnings and risk assessments. In the meantime, set up independent and efficient, objective and fair, unified supervision of the government disclosure mechanism and supervision complaint mechanism, in order to improve the accuracy and targeting of supervision, provide comprehensive assistance for citizen judicial relief.
Improve comprehensive administrative filing review and risk assessment system. Timely reversal of the regulatory concept of facial recognition technology is the key to task regulation, not blindly passively remove the danger, but more actively prevent risks. From the perspective of the review standards for government agencies, it is necessary to consider whether the application of facial recognition technology is within the scope of legal responsibilities, whether the application content and procedures are legitimate, whether the application scope and methods are commensurate with the purpose, whether the purpose of facial information collection is justified, and whether the collection type and scale adhere to the "minimum and necessary principle". In terms of the review content of commercial entities, it is necessary to consider whether the users have the right to know, consent, choose and pursue legitimate interests, whether the operation subjects have the qualification conditions stipulated by the state, whether the technical ability and management ability of the information enterprises can be competent for the collection and processing of facial data, and whether the manual review of the automated procedure meets the needs.

(3) Improve the post-administrative punishment and guidance mechanism

Improve the supervision power responsibility mechanism and relief channels. To date, the content of administrative relief Law has still limited to regulating administrative disputes in the physical field, and it has not yet responded to brand new disputes in the digital field space in a timely manner, and the scope of accepting cases only covers general administrative legal acts instead of administrative factual acts. In addition, key factors such as administrative procedure rules, relief channels and responsibility mechanisms in information collection needs to reform and perfect. Although the Personal Information Protection Law has initially stipulated a public interest litigation system for personal information protection, it cannot completely solve endless personal information disputes in real life. For that reason, government departments should rationally weigh the pros and cons of both sides, set up a sound responsibility investigation system, and promptly investigate and punish those who engage in illegal activities in the process of applying facial recognition technology. Further, the relevant departments should formulate regulatory schemes and paths for the application of facial recognition information, and form public opinions through multi-subject participation and interaction, develop practical and operable implementation methods, and achieve the industrialization of personal information

use and the purpose and function of digital human rights protection. In addition, the people's Procuratorate, consumer organizations prescribed by law and the National Cyberspace Affairs Departments should jointly build an administrative public interest litigation system on the basis of the public interest litigation system, and urge government departments to truly administer by law and maximize government functions.

Differentiated administrative penalties should be strengthened. Government administrative organs should formulate specific administrative punishment measures and increase the intensity of administrative punishment, taking into account the overall factors such as the scope of the risk and the extent of the harm, the frequency of the enterprise's violations of laws and regulations, and the corresponding remedial measures taken by the enterprise. For the information developers and processors who abuse or even illegally process facial information should be given warnings, fined, ordered to correct within a time limit, ordered to delete, removed facial recognition information and other administrative penalties. For enterprises with particularly serious circumstances, deeply subjective malignancy, particularly severe social impact, and causing significant losses to the interests of the state and the people, more severe administrative penalties such as large fines, blacklisting, and prohibition of entering the market should be imposed, so as to produce a strong deterrent effect.

Promote the formation of self-discipline conventions by administrative regulations. As technology continues to advance, industry standards will change, so the rules of self-regulation becomes the best way to supervise the use of facial recognition information. Relevant industries comply with laws, regulations, technical standards and specifications can not only help government departments reduce unnecessary regulatory costs, but has a high degree of flexibility. As far as the facial recognition industry is concerned, the relevant subjects should form a new pattern of collaborative governance of internal leadership that the industry leads internally and the government supervises externally, and form self-regulatory norm for the use of facial recognition technology. Specifically, the government administrative organs should take the lead in establishing a punishment mechanism for the non-standard application of facial recognition technology, improve the administrative accountability mechanism, encourage the industry to build self-regulatory organizations and form self-regulatory conventions, and should also give the industry self-regulatory organizations a certain range of pre-access approval power and post-evaluation punishment power through a series of supporting support such as policies and systems. This can not only inhibit the abuse of facial recognition technology from the source of chaos, but release greater energy for the steady development of the industry.

Strengthen public participation and social oversight. Social supervision is the most appropriate and efficient way for information subjects to protect their rights. The establishment of social supervision and reporting channels under the multi-party cooperative supervision mechanism is convenient to obtain the demands of information subjects in a timely manner, and provide reasonable and effective handling ways and feedback opinions. To avoid exaggerating one aspect and resulting in cognitive bias, the public should be aware of the importance of self-protection and the measures taken by the state to protect personal information from large amounts of online platforms and individuals who disclose personal information. That is, not unconsciously indulge in the convenience, security and efficiency it brings, but pay more attention to the privacy and security risks it contains. If the relevant subject is found to have violated laws and regulations, or its own rights and interests have been infringed, the subject should actively complain, report or file a lawsuit.

Conclusion

In the digital age, facial recognition technology is a double-edged sword. While improving the efficiency of social operation, enhancing the user service experience, and stimulating innovation potential and vitality, it also poses a major threat to industrial security and social stability. However, as the so-called "pay a person back in his own coin", big data and informatization can also become the governance means to deal with the challenges and risks brought by economic globalization. Only by continuing to improve the administrative legal protection of the application of personal identification technology and citizen identity information, further elaborating relevant provisions, clarifying the legal principles and obligations that each subject should abide by, and distinguishing the focus of administrative laws and regulations in different application scenarios can we accomplish data security and prevention control tasks, effectively protect citizens' personal information security, make the operation of government power more standardized, orderly, smooth and efficient, and make the operation of society more open, fair and just.

References

[1] Chen Wei, Song Kunpeng, (2020). Investigation on the Mode of Joint Prevention and Treatment of Telecom Fraud Crimes Relying on Personal Information: An Empirical Analysis based on 400 judgments in a Province, Chinese Criminology Review, No. 2, p. 53.

[2] Gao Zhongxun, (2021). "Multi-level" legal norms for protecting facial recognition Information, Procuratorial Daily, September 8.

[3] Guo Chunzhen, (2020). Governance of Facial recognition technology Application in the era of Digital Human Rights, Modern Law Science, No. 4, p. 31.

[4] Jiao Yanling, (2022). The Identification of Tort Liability for Facial Recognition, Social Sciences in Chinese Higher Education Institutions, No.2, pp. 118-119.

[5] Li Zhenlin, (2022). Criminal Law Regulation of Illegal acquisition or Use of Facial Recognition Information", Journal of Soochow University (Philosophy and Social Sciences Edition), No. 1, p. 75.

[6] Liu Xuetao, (2018). Analysis of Administrative Law Protection of Personal Information in the Era of Big Data: Connotation, Dilemma and Path Selection", Journal of Beijing University of Posts and Telecommunications (Social Science Edition), No.6, p. 29.

[7] Lu Qing, (2019). The normative construction of consent rules in Personal Information Protection, Wuhan University Journal (Philosophy & Social Science), No. 5, pp. 123-126.

[8] Ma Changshan, (2022). Introduction to Digital Rule of Law, Law Press 2022, p. 74.

[9] Ma Changshan, (2019). The Fourth Generation of Human Rights and Its Protection in the Context of Smart Society, China Legal Science, No. 5, 2019, pp. 5-8.

[10] Pan Linqing, (2020). Technical Incentives, Theoretical Basis and Normative Structure of Legal Protection of Facial feature Information, Journal of Northwest Minzu University (Philosophy and Social Sciences), No. 6, pp. 77-80.

[11] Sun Di, (2022). Liu Xuetao, Government Responsibility and Administrative Law Regulation of Citizen Identity Information Leakage: Against the background of the COVID-19 epidemic, Credit Investigation, No. 9, p. 39.

[12] Xu Yandong, (2015). The moral metaphysics of “Face”-- A Study of Agamben’s Philosophy of “Face, Man, and Thing “, Philosophical Trends, 2015 (2), pp. 19-20.
[13] Zhang Tao, (2021). Application Risk and Legal Control of Facial recognition Technology in government Governance, Henan Social Sciences, No. 10, pp. 51-53.
[14] Zhang Yong, (2021). Legal Protection of Personal Bioinformation Security -- Taking Facial Recognition as an example, Jiangxi Social Sciences, No.5, pp. 166-167.