World Scientific Research Journal Volume 8 Issue 10, 2022
ISSN: 2472-3703 DOI: 10.6911/WSRJ.202210_8(10).0025

Face Information Technology Recognition Application of Legal Regulations

Xinru Song[1, a]

[1]School of Law, Anhui University of Finance and Economics, Anhui, China

[a]1663007033@qq.com

Abstract

The human face, as a kind of biometric information, has always been an important information carrier for human beings to carry out cognitive social activities. In recent years, with the development of sensor technology, artificial intelligence technology and big data analysis and processing technology, the unique and common information carrier of the face has gradually evolved into a part of personal digital information, that is, face recognition information or data. Compared with other biometric information, face recognition information shows a high degree of sensitivity, diverse, concealed and flexible collection methods, and improper use may bring unpredictable risks to the personal and property safety of citizens. In addition, face recognition technology also faces unique regulatory difficulties, and in some scenarios, even has moral and ethical concerns. In the face of the wider popularization of face recognition technology, under the premise of strengthening supervision and ensuring the security of personal information, promoting the legal and compliant circulation of face recognition information is the best way to guide the development of the industry.

Keywords

Face recognition information; Personal information protection; Give consent; The principle of imputation.

1. INTRODUCTION

In October 2019, the service contract dispute between Guo Bing and Hangzhou Wildlife World Co., Ltd. attracted great attention from all walks of life and was called China's "first face recognition case".

After trial, the court of first instance found that Hangzhou Wild Animal Park's change of fingerprint entry method during the performance of the contract to face recognition was a breach of contract to unilaterally change the content of the contract, and ordered it to delete the facial feature information, including the plaintiff's photo, and compensate Guo for the loss of contract benefits and transportation expenses.

The privacy security and legal regulation of face recognition technology triggered by this case have become a hot topic of social discussion. Face recognition technology is one of the most widely used artificial intelligence technologies at this stage, but from the perspective of privacy and security, the legal risks caused by the basic technical attributes of the face recognition mechanism will be a major challenge in this field that cannot be ignored.

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202210_8(10).0025

2. THE CONCEPT OF FACE RECOGNITION INFORMATION

Face recognition technology refers to the technology that converts the detection image of a natural person into a digital model or template of a face. It has three basic functions of detecting, verifying and recognizing: recognizing the facial information present in the image, verifying the identity related to the confirmed facial information, and matching the image of the unknown face with a known natural person. Compared with other biometric technologies such as fingerprint collection and vein recognition, face recognition technology has the advantages of non-contact, strong interactivity, difficult to be stolen and efficient.

The conceptual distinction between face and face recognition information is relatively clear, the former refers to the physiological image of the person's face, and the latter refers to the personal data obtained through specific data processing of the physiological characteristics of the face of the natural person, and the face image of the unique identity of the natural person can be generated in the model software through such data. That is to say, face recognition information is first used to collect and detect the face image by sensors, and then the collected face information is extracted from the feature points, and finally through computer software for data processing, and the face becomes a set of "numbers" coded in the digital world. The purpose of face recognition is to use this set of data for real-life face acquisition, comparison, coupling, and correction to achieve recognition and comparison between digital models and real faces.

After the promulgation of the Personal Information Protection Law, Article 4 clearly stipulates: "Personal information is all kinds of information related to identified or identifiable natural persons recorded electronically or otherwise, excluding information after anonymization." "Not only has the provisions of the Civil Code been refined, but also the protection of personal information has gradually been carried out under the new legal system for the protection of personal information with the promulgation of the Law: specifically, the definition of the concept of personal information, the collection, storage, processing, deletion and other operations of information collection, storage, processing, deletion and other operations are generally summarized as "processing", and sensitive information is distinguished from general personal information and different processing rules are formed.

3. THE CURRENT SITUATION AND EXISTING PROBLEMS OF FACE RECOGNITION INFORMATION PROTECTION IN CHINA

The Personal Information Protection Law came into force on November 1, 2021, marking a new, systematic and further legislative decision on the purpose, scope, rules, and methods of personal information protection in China under the legal system of personal information protection in the digital context. Under the system of personal information law protection, the laws and regulations related to face recognition information are still scattered, and the problems of insufficient coherence and coordination between laws and regulations, and the low degree of integration between other normative documents may make it more difficult for the information subject to obtain effective legal guidance or remedies in judicial practice as the infringed.

Therefore, at present, we should strengthen the research on the legal protection of face recognition information, so as to obtain a clearer protection path under the new legal system of personal information protection, so as to find a more accurate and detailed basis for protection, so that legal governance can keep pace with the development of information technology. In the content of relevant legal protection, there are also many problems, which are embodied in the following aspects.

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202210_8(10).0025

3.1. The Misunderstanding of The Relationship Between The 《Personal Information Protection Law》&《Civil Code》 Affects The Specific Application

Because before the promulgation of the Personal Information Protection Law, almost all case disputes involving the protection of personal information relied on the special chapter provisions on privacy and personal information protection in Chapter VI of the Civil Code, administrative regulations such as the Measures for the Administration of Internet Information Services, the Provisions on the Online Protection of Children's Personal Information and other departmental rules and other normative documents to jointly resolve the cases, until the promulgation of the new law, and at the same time combined with the amendments made by the Supreme People's Court to the Provisions on the Causes of Action in Civil Cases, the "cause of action for personal information protection disputes" was finally obtained This means that the protection of such cases can be carried out under the new legal system for the protection of personal information, but the academic circles have different views on its relationship with the Civil Code, and some views are prone to misunderstandings, which ultimately affect the specific application of law enforcement and justice.

Some people believe that because the Previous Civil Code has already provided for the concept and fair use of personal information, the provisions of the Personal Information Protection Law that have been promulgated later should be developed under the system of the Civil Code, so the above scope has a relationship between general law and special law. This view is more one-sided and backward, because it ignores the status of the Personal Information Protection Law as a comprehensive legislation, and limits its application to the Civil Code without paying attention to its new protection system.

Others argue that the Personal Information Protection Act is public law in nature and has no relationship with the private law rules of the Civil Code. In fact, the rights and interests of personal information have been protected by both public law and private law, and the confirmation of personal information rights and interests is completed by the Civil Code, and it is impossible to achieve full protection of the rights and interests of information subjects through public law, so it is not possible to ignore or even ignore the protective role of private law in the Personal Information Protection Law. This view will divide the relationship between the two laws, and will also ignore the coherence of the two laws in resolving disputes, and increase the difficulty of trial based on complex circumstances when analyzing cases in judicial practice, which ultimately affects the accuracy of the court's judgment.

Therefore, to solve the misunderstanding of the relationship between the two laws, we should examine the similarities and differences of the legislative purposes, systems, and relevant provisions of the two from a more macroscopic perspective, sort out the relationship between the two, and obtain specific and applicable solutions.

3.2. The Rules of Notification Consent Are Challenged

As the basic rules to solve the problem of face recognition information collection, the notification consent rule or informed consent rule is mainly to protect the information self-determination rights enjoyed by the information subject, and with the gradual implementation of the Civil Code, the Cybersecurity Law and the Personal Information Protection Law, the way of information collection and processing is restricted in the way of giving the information subject rights.

3.2.1.Express consent and implied consent

Consent means that the user clearly knows the scope, method and purpose of the data enterprise to collect facial recognition information. At present, there are two ways to consent when collecting face recognition information, namely explicit consent and implied consent. The provisions of explicit consent can be corresponded to in the Personal Information Protection

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202210_8(10).0025

Law and the Provisions: the collection of face information requires the written consent of the information subject, which is embodied in the face recognition information collection agreements signed by many APP application platforms and users. Implied consent means that the information subject can express his consent by inaction, and its implied consent should be made when the information subject should realize that his or her face information will be collected.

3.2.2.The platform uses "implied consent" to cause the failure of the notification consent rules

Although the information subject is the key to authorization, even under the premise of legally collecting information, it is difficult for the user to fully know how the enterprise will carry out data analysis activities in the future when authorizing for the first time, which makes some platforms as the processing subject use the so-called "implied consent" clause in the service agreement to cause the failure of the notification consent rule.

It is not difficult to see that the platform may formulate the agreement after considering the cost, energy, delay in transaction opportunities, etc. of re-entering the written consent, and only perform the notification obligation at the beginning of the information collection and processing based on the consideration of interests, but after obtaining the initial authorization of the information subject, the practice of not taking the explicit consent method of written consent itself has violated the statutory notification obligation, and then uses "implied consent" to replace "deemed consent" The practice of the clause makes the notification and consent rule fail, which will also cause most of the public who directly click the "agree" button to question the credit of the platform and the use of the information, causing panic about not knowing how to deal with their face recognition information, such as fear that their information is illegally bought and sold for crimes, and they are trapped in loan sharks.

3.3. Processing Entities Use Technology to Bypass the Notification Consent Rules

In practice, with the development of face recognition technology, compared with the information subject, data companies as a strong subject, often abuse their information collector, processor identity, and constantly improve the technical level, has been able to use face information non-contact, non-sensor recognition technology can be exposed to the face recognition camera face recognition information for capture, in order to later analysis and processing, this operation directly bypasses the rules of notification and consent, serious violation of the law. Nowadays, this situation has gradually become rampant, not only can the crawling operation be realized under the camera that can be seen everywhere in public, but even our usual short videos, photos and other channels have become the source of illegal access to face recognition information by data companies. As a result, the voices of doubt have followed, and the public is not only worried about the infringement hazards of data companies in the process of collecting and processing face recognition information, but also about the legality of public authorities based on the protection of public interests in collecting and processing information, so it is imperative to improve the content of the rules for informing consent.

4. SUGGESTIONS FOR IMPROVING THE LEGAL SYSTEM FOR THE PROTECTION OF FACE RECOGNITION INFORMATION

4.1. Clear Conceptual Definitions to Suit Specific Applications

Combined with the rapid development of the current face recognition technology and the many illegal processing risks that accompany it, the infringement cases that appear in practice will gradually increase, and the risk of illegality will gradually increase, which will make more and more information subjects begin to seek legal ways to solve the problem, and the definition of face recognition information in the Personal Information Protection Law will indeed make it impossible to obtain accurate identification standards in the process of handling cases,

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202210_8(10).0025

especially for the question of whether the information generated by the combination of emerging technologies and faces should be protected by the Law. As well as whether the subsequent application of the notification and consent rules and the principle of tort liability have misunderstandings, so face recognition information should be clearly defined in the Personal Information Protection Law or the Provisions.

Drawing on foreign countries and referring to the degree of protection that China should have for the current face recognition information, it is recommended to adopt the method of "definition enumeration and exclusion". In the enumeration method, the inexhaustible enumeration is adopted, and the connotation is elaborated in conjunction with the first part of this article: one is the original identification information collected directly by the use of technology, and the other is the re-identification information containing the identity information, whereabouts and other information generated by the analysis and retrieval processing of the technology, which can expand the scope of protection of the law accordingly, and leave a legal basis for infringement cases such as identity information generated in the future. In addition, relevant face recognition information that is not protected by the Personal Information Protection Law should be excluded in accordance with the Personal Information Protection Law, such as "anonymized information" stipulated in the first paragraph of Article 4 of the Personal Information Protection Law, which is not protected by the Law, because after anonymization, a specific natural person cannot be identified and cannot be restored. In summary, the face recognition information in this paper attempts to define: the face information obtained by recognizing the face of a natural person through face recognition technology. This includes, but is not limited to, the original identification information collected using technology and re-identification information including identity information, whereabouts, etc. generated by processing such as analysis and retrieval by using technology. Face recognition information after anonymization is not included.

4.2. Improve the Rules for Informing Consent

4.2.1. Establish differentiated rules for informing consent

Differentiated rules for informing and consenting should be established based on the needs of different collections and uses of face recognition technology for "anonymization" and "de-identification", and the subjects, scenarios, and uses of the technology.

For private interests such as data enterprises, the purpose of collection and processing is mostly to pursue interests, which is different from the starting point of public authorities, so it should be different from public authorities when establishing rules for informing and consenting. For example, when performing the rules, enterprises should fully inform the information subject of the content of the standard terms and service agreements, and should use eye-catching fonts and logos to make specific enumerations of the purpose, use, whether the face recognition technology is restored to "anonymized information" after processing, and the adverse effects that may be caused, such as whether to carry out personal identification, activity trajectory, sentiment analysis, sentiment calculation, etc., to avoid abstract words such as "including but not limited to". At the same time, it should also be listed and provided that the user does not agree to use the face recognition technology to provide other equivalent services to ensure that the information subject is treated unfairly and differently.

4.2.2.Adopt multiple notification procedures

The multiple notification procedure may require the platform to set up a multi-layer notification procedure under the terms of informed consent when registering with the user's APP, and complete the notification operation through multiple reminders such as voice prompts plus video demonstrations and eye-catching red characters, so as to avoid many users from clicking the confirmation button for simplicity when registering without looking, thus bearing

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202210_8(10).0025

the adverse consequences of "mistakenly believing consent"; Avoid undesirable technology platforms that only make specific enumerations during the initial information collection and processing, use "tacit consent" to obtain reauthorization after obtaining the authorization of the information subject, resulting in adverse consequences, and reduce the illegal application of intrusion into citizens' information and theft of information to commit illegal crimes. In addition, using specific enumeration methods to set different options, information subjects can formulate satisfactory personalized terms in a freely chosen way, so as to deepen their understanding of the matters of notification and consent and meet the information processing needs of different users.

5. EPILOGUE

Face recognition technology provides extensive technical support for the intelligent transformation of social governance. However, the personal information corresponding to face recognition technology covers multiple legal benefits, and if there is no scientific and effective legal regulation, face recognition technology will inevitably be abused, and it will inevitably induce complex and diverse social risks. At present, China's legal regulation of face recognition technology lags seriously behind the application of this technology, which is specifically manifested in the unclear definition of the attributes of rights in the application of face recognition technology, the inconsistent legislative purposes, the pertinence of legal regulations is not strong, and the after-the-fact regulatory logic of the law itself. Therefore, grasping the opportunity of comprehensive legislation, refining regulations for different scenarios, clarifying the similarities and differences in the rights and responsibilities of all parties, and achieving collaborative co-governance are the directions for maintaining personal information security and ensuring the intelligent transformation of social governance。

ACKNOWLEDGMENTS

Anhui University of Finance and Economics Postgraduate Research and Innovation Fund Project " Face Information Technology Recognition Application of Legal Regulations" (Project Approval Number: ACYC2021091).

REFERENCES

[1] Zhong shao.Gao, Legal regulation of face recognition information processing behavior, Learning Forum,Vol. 43 (2022) No.1, p.132.

[2] Chen kai.Jing, A review of face recognition technology based on deep convolutional neural networks, Computer applications and software, (2018) No.1, p.223.

[3] Ling.Hu, Brushing faces: identity systems, personal information and legal regulations, Jurisconsult, (2021) No.2, p.41-56.

[4] FuPing.Gao, Personal information protection: from personal control to social control, Legal Studies, (2018) No.3, p.84-101.

[5] Ling.Lin, "Notification of consent" and "data utilization" rules in face recognition information protection, Contemporary communication, (2022) No.2, p.110.

[6] Miao.Cai, Construction of informed consent rules in the collection of facial information, Network security technology and application, (2022) No.2, p.139.