HiLL PUBLISHING

Journal of Humanities, Arts and Social Science, 2023, 7(10), 2053-2057
https://www. hillpublisher. com/journals/jhass/
ISSN Online: 2576-0548
ISSN Print: 2576-0556

The Dilemma and Legal Protection of Consumers' Face Recognition Information Under Face Payment

Meiyan Liu

Dalian Ocean University, Dalian, Liaoning, China.

How to cite this paper: Meiyan Liu. (2023) The Dilemma and Legal Protection of Consumers' Face Recognition Information Under Face Payment. *Journal of Humanities, Arts and Social Science*, 7(10), 2053-2057. DOI: 10.26855/jhass.2023.10.026

Received: September 30, 2023
Accepted: October 29, 2023
Published: November 27, 2023

***Corresponding author:** Meiyan Liu, Dalian Ocean University, Dalian, Liaoning, China.

Abstract

The face payment industry relies on the advancement of face recognition technology, and currently, face payment is being extensively utilized across various industries. While it brings convenience to consumers, it is also accompanied by many legal risks, such as the confusion between face recognition information and general personal information, as well as the difficulty for consumers to participate in the formulation of rules as information subjects. In order to address various challenges, it is necessary for legislation to grant special status to face recognition information and provide special protection. The judicial system should also explore the concept of security guarantee obligation and the principle of implementing responsibility. Additionally, law enforcement agencies should prioritize the effective coordination between the government supervisory department's pre-event, during-event, and post-event supervision to ensure comprehensive oversight. This will help safeguard the rights and interests of consumers' face recognition information. Under the premise of continuously improving laws and regulations, it is necessary to strengthen and enhance the obligation of security protection for consumers' face recognition information. Additionally, efforts should be made to improve consumers' awareness of self-protection and provide accurate legal guidance for both operators and consumers.

Keywords

Face recognition technology, face recognition information, face payment, security guarantee obligation

1. Overview of face payment

1.1 Principle of face payment

The emergence of face payment relies on the rise of face recognition technology, and it is a product of face recognition technology in the payment field.

Its basic principle is to determine personal identity by comparing biometric information collected by terminal hardware (such as cameras and cell phones) with personal information stored in the cloud, so as to activate the association between face recognition information and payment system and complete contactless authentication and payment.

1.2 Development history of face payment

In July 2013, Finland's Uniqul launched the world's first payment platform based on face recognition technology, marking the official application of face payment in various fields. on February 21, 2017, the authoritative academic magazine MIT Technology Review selected face payment as one of the world's top ten breakthrough technologies in

2017. On July 8 of the same year, the State Council clearly pointed out in the "Notice on the Issuance of the Development Plan for a New Generation of Artificial Intelligence" that it was necessary to seize the major strategic opportunities for the development of artificial intelligence, build a preemptive offensive of artificial intelligence in China, and accelerate the creation of a science and technology powerhouse. This document directly unveiled the prelude to domestic face payment. Alipay and WeChat then launched face-brushing devices and successively landed in merchants nationwide, and face-brushing payment has involved all walks of life.

2. The dilemma of consumers' face recognition information in face payment

2.1 The confusion of face recognition information and general personal information

Face payment is a product of face recognition technology in the payment field, and it relies on face recognition information as its foundation. In terms of legislation, the Civil Code - Personality Rights only classifies biometric information as personal information, without making any further distinctions. The Network Security Law also fails to clearly differentiate between sensitive personal information and general personal information. As a result, face recognition information can only be classified as general personal information and afforded protection (Diao Shengxian & Jiang Yin, 2022). There is a legal lag in the face payment industry, which is becoming increasingly mature. However, on August 20, 2021, the Law of the People's Republic of China on the Protection of Personal Information (hereinafter referred to as the "Personal Information Protection Law") was formally implemented on November 1, 2021, after being considered and adopted by the 30th meeting of the Standing Committee of the 13th National People's Congress (Diao Shengxian & Jiang Yin, 2022). The legislation provides clearer legal support for the protection of personal information, including face recognition data. It formally includes biometric information as a form of sensitive personal information at the legislative level. However, there are still unclear aspects, which result in challenges in the judicial field. These challenges include a fragmented legal basis, limited protection options, and difficulties in determining infringement and avoiding cases related to face recognition.

2.2 Consumers as information subjects find it difficult to participate in rule-making

Under face payment, operators will inform consumers of the possible risks of face payment in a way that consumers can be informed and obtain their informed consent, which reflects that consumers can handle their own personal information independently and fully respect their right to informed consent. Take Alipay as an example, when consumers open the face payment, the system will automatically pop up the General Rules for Biometric Services, which is essentially a format clause generated by the operator for signing a sales contract with consumers, and is a clause unilaterally formulated by the operator for repeated use without consultation with the other party, and most of the operators providing face payment in the market at present only have the right to informed consent of consumers on the majority of the operators in the market currently provide face payment services have only superficial consent, because consumers only have two options to agree and disagree when facing the face payment services provided by the operators, and there is no way to enjoy the services once they refuse. As a result, most consumers are forced to agree to the format terms provided by the operator, which limits the opportunity for equal negotiation between consumers and the operator. At the beginning of Alipay's General Rules, it is explicitly mentioned that the collecting subject may contact the information processing platform to obtain an explanation if he/she has questions about the rules. While this approach provides the possibility of communication with the Alipay platform, it only expresses the obligation to explain. It lacks a way for both parties to participate in the formulation and change of the terms. At the same time, the provision does not provide a specific way to consult, which makes it even more difficult for the consumer, who is on the weaker side of the transaction, to participate in the development of the contract. This situation becomes even more prominent when biometric information becomes a means of payment, and therefore requires more perfect regulations and safeguards.

3. The improvement of legal protection of consumers' facial recognition information under face payment.

3.1 Give a special status to face recognition information

Face recognition information is particularly special and important under face payment, but the current domestic legislation does not give special status to face recognition information. In the Civil Code, the Net Security Law, the

Consumer Rights Protection Law, and other laws, its status is no different from that of general personal information. The Judicial Interpretation of Face Information clearly expresses the protection object as "face information", and limits it to "using face recognition technology to process face information" and "processing face information generated based on face recognition technology ". In fact, the face information in both cases is used for identification and belongs to the "biometric information" in the Personal Protection Law and the Civil Code, plus the definition of personal information in our legislation also adopts the "identification standard", so it is suggested that the legislation will Therefore, it is recommended that the legislation should refer to "face information" as "face recognition information", and is classified as sensitive personal information and important data. This can avoid expanding the protection of face information not used for identification. The efficiency, simplicity, and convenience of face swipe payment are loved by the majority of consumers. Still, the risks involved in face recognition information leakage and illegal use have been ignored. Giving face recognition information a specific legal status can give it more attention and importance, thus improving consumers' legal awareness in disguise.

3.2 Special protection for face recognition information on the basis of granting it

3.2.1 Fully implement the principle of informed consent by combining the dynamics of specific scenes

The principle of informed consent is that information processors should protect the right to information and obtain consent when collecting personal information of information subjects, which is the basis and premise of handling personal information. However, in the field of face payment, the principle of informed consent is often only superficial, and it is difficult to truly protect the rights and interests of consumers. In reality, there are many forced consent clauses, and a consumer's right to information self-determination is often subordinated to the dominant operator. At this point, it is necessary to emphasize the dynamic nature of the right to informed consent, i.e., the ability to withdraw consent at any time according to changes in the situation, rather than the original mechanical authorization for life. Dynamic implementation of the right to informed consent can ensure that consumers are fully informed and agree, and the adoption of dynamic consent can improve the effectiveness of consent authorization so that consumers can truly participate in the rules.

3.2.2 Try to introduce third-party certification bodies

Given the gap between the status of consumers and operators, it is difficult for consumers in a disadvantaged position to participate equally in rule-making. In reality, even if consumers question the platform, they only provide a channel to explain, so the introduction of a third-party certification body is an effective channel and means to provide consumers with the right to participate in rule-making and information self-determination. First, the third-party certification body can screen and retain valid opinions from consumers and then negotiate on an equal footing with the operator platform as a representative, and provide real-time feedback to consumers on the results of the consultation, which greatly protects consumers' right to informed consent. Secondly, for the post-facto situation change, consumers need to exercise the right of deletion, due to the face recognition information having non-contact, easy-to-copy, and spread characteristics, the consumer's right of deletion is difficult to implement, in order to further protect the realization of the consumer's right of deletion, can introduce a third-party certification body to review and assume the real results of the deletion or change of face recognition information and assume the corresponding certification responsibility. Authentication by a third-party authentication agency can effectively reduce the disputes and controversies caused by the deletion or alteration of information. The cost of identification for the third-party certification agency should be borne by the infringer or the violator to increase its illegal cost.

3.2.3 Raise the legal awareness of consumers

Face payment is a highly developed technology, and its convenience and efficiency meet the needs of the future market. However, during the operation of this service, some problems different from traditional payment are gradually exposed. This requires the legal awareness of consumers to follow to improve in order to avoid harm under the face payment. The most important channel to improve legal awareness is to come from the publicity of public security organs and government agencies so that citizens can be more aware of the importance of face recognition information.

3.3 Constructing a coordinated protection path of legislation, justice, and law enforcement

3.3.1 Improve National Legislation

Article 14 of China's Consumer Rights and Interests Protection Law stipulates the right to the protection of

consumers' personal information. Article 29 stipulates the principles of collection and use of consumers' personal information by operators. Additionally, Articles 50 and 56 outline the legal responsibilities that operators should bear when infringing on consumers' personal information. However, the Consumer Rights and Interests Protection Law lacks comprehensive and detailed regulations for the protection of consumers' personal information, which is insufficient for the legal regulation of face payment. The legal regulation of facial payment is still far from sufficient. In order to enhance the legal regulation of biometric information, China's legislation can take into account the personal information protection principles of the European Union and the United States (Jiang Shuxu & Hu Dan, 2020). Such provisions can be established to define "biometric data" and incorporate it into the law. Biometric data, including biometric data as special types of personal data, is subject to specific regulations. These regulations include "prohibited processing," "express consent," and "legal necessity" as special sensitive types of personal data. These principles apply to the processing of special sensitive types of personal data, such as biometric information.

3.3.2 Judicially explore the path of security obligations and the principle of lawful implementation of responsibilities

(1) Establishment of punitive damages system

In judicial practice, consumers as a whole are often in a vulnerable position, and it is difficult to safeguard consumers' personal information rights by relying solely on compensatory liability. Therefore, it is necessary to establish a punitive damages system. On the one hand, it can increase the cost of infringing on the operator's rights in order to achieve a deterrent effect. On the other hand, when consumers are solely responsible for defending their rights, the cost of doing so can far exceed the anticipated benefits. Implementing a punitive damages system can effectively harness consumers' enthusiasm to protect their rights and motivate them to proactively initiate lawsuits in order to safeguard their interests.

(2) Improve public interest litigation participation channels

The leakage or illegal use of biometric information by an unspecified majority of consumers may infringe on public legal interests such as social interests or national security. Therefore, it is recommended that Article 14 of the Regulations of the Supreme People's Court on the Application of Law in Civil Cases Concerning the Use of Face Recognition Technology in Handling Personal Information should further clarify the conditions, compensation standards, and refund methods for public prosecutors to file public interest litigation against infringement of consumers' face recognition information. This will achieve the effect of "leading from point to point" comprehensive governance, and provide a better institutional guarantee for the protection of consumers' personal information. In addition, individual consumers should also actively file class action lawsuits or report the situation to the relevant departments, so as to initiate public interest litigation to protect their rights and interests. Third-party certification agencies should be encouraged to undertake identification work such as the deletion and change of face recognition information and bear the corresponding certification responsibility. The appraisal cost should be borne by the infringer or the defaulter to increase its illegal cost.

(3) Clarify the principle of attribution of face recognition information

The principle of attribution of responsibility in the face of such personal information infringement cases in face swipe payment takes the principle of fault, but consumers as a vulnerable group find it difficult to obtain evidence, which will inevitably make the consumers' right to judicial remedy fall short. Based on the protection of consumers' face recognition information, the principle of no-fault imputation for face recognition information infringement can better compensate for the weak evidential position of consumers as information subjects. Only by increasing the burden of proof of the enterprise will the enterprise be urged to better implement the security obligations in the business activities of face recognition payment and thus reduce the occurrence of face recognition information infringement.

3.3.3 Strengthen the supervision of the government

The current situation of domestic law enforcement is that the government lacks specialized agencies to regulate the behavior of the face payment industry, and the process of government departments lacks coherence for supervision before, during, and afterward.

(1) Strict review of corporate qualifications

In order to enhance pre-market supervision, a system of pre-review market access can be implemented. This means that enterprises offering facial information services should submit relevant information in advance, including usage boundaries, purposes, storage methods, time limits for use, deletion methods, emergency response capabilities, etc.

(Jiang Shuxu & Hu Dan, 2020), and approved by the relevant government departments before they can operate. This can protect the rights and interests of consumers and prevent the abuse and unauthorized disclosure of personal information by enterprises.

(2) Strengthen daily inspection efforts

The government department's strength for the review in the matter should not be weakened by the completion of the prior review, and the phenomenon of access to life should be avoided. In the process of operators providing face payment services, the means and purposes of collecting face recognition information should be regularly reviewed for legality and corrected in a timely manner, and records should be kept on the review.

(3) Improving the post-event recovery and punishment system

Once the government supervisory department finds that the operator has leaked consumers' face recognition information, it should promptly request the operator to explain the infringement and take the initiative to report the scope of the number of leaks, the amount of information, and the measures taken or being taken. The supervisory department shall take remedial measures and hold the relevant operator accountable for the nature of the incident, the circumstances, and the severity of the damage.

(4) Determining a single supervisory authority to centralize administrative supervision

Because the protection of face recognition information involves the scope of responsibility of many departments, the reality may produce the problem of unclear authority and responsibility, so it should learn from foreign legislation to adjust the main body of supervision, unified supervision responsibility department, so as to enhance the administrative supervision and relief target.

4. Conclusion

When utilizing facial information, enterprises should clearly define the scope and purpose of its usage, and adhere strictly to the requirements for storing information to guarantee its security. In addition, enterprises should also give comprehensive consideration to the time limit for information use, methods of deletion, and emergency handling capabilities, and keep detailed records of all information handling activities to ensure the security of information.

References

Adjabi, I., Ouahabi, A., Benzaoui, A., Taleb-Ahmed. A. Past, Present, and Future of Face Recognition: A Review. Electronics 2020, 9, 1188. https://doi.org/10.3390/electronics9081188.

Diao Shengxian, Jiang Yin. On the legal protection of face recognition information: a review of the "first case of face recognition" in China [J]. Journal of Chongqing Institute of Science and Technology (Social Science Edition), 2022(06):19-31.

Jiang Shuxu, Hu Dan. Legal protection of consumers' personal information under swipe payment [J]. Journal of Shanxi Academy of Political and Legal Management Cadres, 2020, 33(04):43-46.

Oloyede, M.O., Hancke, G.P. & Myburgh, H.C. A review on face recognition systems: recent approaches and challenges. Multimed Tools Appl 79, 27891-27922 (2020). https://doi.org/10.1007/s11042-020-09261-2.

Rapcsak, S.Z. Face Recognition. Curr Neurol Neurosci Rep 19, 41 (2019). https://doi.org/10.1007/s11910-019-0960-9.