DS NEWSLETTER savoir, faire

NEWSLETTER - LEGAL INFORMATIONS

PROPOSED BY DS AVOCATS

"Face Pressure": what's new about facial recognition in 2020 and 2021?

ASIE

INTRODUCTION

Facial recognition is a biological technology based on human facial biometric features. It relies on the support of hardware, algorithm and data to realize the function of facial recognition. Due to its contactless nature and the popularity and development of hardware integrating facial recognition technology, facial recognition is becoming more diversified and matured. At present, China is expected to become the world's largest «playground» for facial recognition technology.

In China, facial recognition is widely used in railway stations, airports and other public places, factories, schools and enterprises, as well as banks, communications, transportation, health and other institutions. It is worthwhile to consider whether the above uses are compliant with the *Cyber Security* Law and other relevant laws and regulations.

Although there is no specific law for facial recognition technology in China, the facial feature data (biometric data) collected via facial recognition technology belongs to the category of personal data and should be regulated by relevant laws on personal data protection. For example, the *Cyber Security Law* and the *Civil Code* stipulate that the collection and use of personal data should follow the principles of legality, legitimacy and necessity, and obtain the consent of the natural person or his guardian.

Moreover, according to the *Civil Code*, citizens have civil rights to their personal data, and illegal collection and sale of personal data without their consent will constitute civil tort. In addition, the *Amendment (9) of Criminal Law* stipulates the crime of infringing citizens' personal data. Buying and selling a certain amount of highly sensitive personal data may also be suspected of criminal offence. In this case, both the buyer and the seller may be suspected of the crime of infringing citizens' personal data.

IMPORTANT UPDATES IN 2020 AND 2021

Although there is no special legislation on facial recognition in China, in order to solve growing issues caused by face recognition technology, some national standards and drafts have been published in recent two years.

- The national standard *Information Security Technology - Personal Information Security Specifications* implemented on October 1, 2020 includes facial recognition data into personal sensitive data. In addition, user portraits or the data related to the facial features, which can identify a specific natural person or reflect the activities of a specific natural person alone or in combination with other data, is also included in the category of personal data.

- The national standard *Information Security Technology - Technical Requirements for Remote Facial Recognition System* implemented on November 1, 2020 specifies the function, performance, as well as the security requirements of the information system that uses facial recognition technology for remote identification on servers.

- The draft of the national standard *Information Security Technology - Security Requirements of Facial Recognition Data* issued on April 23, 2021. It defines the basic security requirements of data controllers, such as taking security measures to ensure the rights of data subjects, including but not limited to obtaining the status of use of facial recognition data, withdrawing authorization, canceling account number, filing complaint , obtaining timely response, etc. In principle, it is not allowed to use facial recognition to identify minors under the age of 14.

The Newsletter is provided for general informational purposes only. Any information contained in this should not be construed as legal advice and is not intended to be a substitute for legal counsel on any subject.

- The *Personal Information Protection Law (Second Draft)* published on April 29, 2021. It points out that for new technologies and applications such as facial recognition, special personal data protection rules and standards shall be formulated, and the national network information department shall coordinate relevant departments to promote relevant work accordingly.

In addition to national level, some local authorities have also issued administrative measures to regulate the collection and processing of personal sensitive data and facial recognition.

- *Tianjin Social Credit Regulations* issued at the end of 2020 explicitly prohibits market credit information providers from collecting biometric data of natural persons.

- *Hangzhou Property Management Regulations (Revised Draft)* issued at the end of 2020 stipulates that property service personnel shall not request owners to be identified through fingerprints, facial recognition or other means based on biometric data to access the utilities.

- *The Social Credit Regulations of Guangdong Province*, effective since June 1, 2021, prohibits the market credit information collection subjects, such as enterprises, to collect natural person's data about religious belief, blood type, disease, medical history and biometric data.

In addition, in some industries where facial recognition technology is widely applied, some restrictive provisions for biometric data have been published.

- The national standard *Personal Financial Information Protection Technical Specification* issued on February 13, 2020 defines the security protection requirements of personal financial data and expands the scope of personal identity data to include personal biometric data, such as fingerprint, face, iris, ear print, palm print, vein, voice print, eye print, gait, handwriting and other biometric sample data.

- *Several Provisions on Automobile Data Security Management (Draft for Comment)* issued on May 19, 2021. It gives a clear definition of the important data of the automobile industry, which includes face, voice, license plate, etc. At the same time, it also stipulates the conditions for collecting personal biometric sensitive data, "only for the purpose of facilitating users' use and increasing the security of the vehicle electronic and information systems can driver's finger print, voiceprint, face, heart rate and other biometric data be collected."

HOW'S THE FIRST CHINESE CIVIL CASE ABOUT FACIAL RECOGNITION?

In April 2019, a tourist subscribed an annual access card of a zoo. For the access, tourists need to provide their personal identity data, their fingerprints and portrait photos according to the service agreement. Later on, the zoo changed its access requirements from fingerprint recognition to facial recognition, and sent short messages to tourists to inform them, requiring them to activate their facial recognition function. However, this matter resulted in disputes between a tourist (who is a professor in law school) and the zoo.

In November 2020, the court made the judgment of the first instance, ordering the zoo to compensate the tourist for the loss of contract interests and transportation expenses, and to delete the biometric data including photos submitted by the tourist previously used for access of the zoo. However, both the tourist and the zoo were not satisfied and appealed.

It took two years to end this first civil litigation related to facial recognition in China. It was finally ruled on April 9, 2021. The court of second instance held that the unilateral change of access mode by the zoo constitutes a breach of contract for which the zoo should bear the responsibility. Moreover, the use by the zoo of the collected photos as facial recognition data goes beyond the initial purpose of collecting such personal data and violates the principle of legitimacy. Therefore, the facial feature data including the photos submitted by tourists should be deleted by the zoo. In view of the fact that the zoo has stopped using the fingerprint identification, which makes the original agreed service mode unable to be realized, the fingerprint identification data of tourists should also be deleted (a requirement added by the court of second instance on the basis of the judgment of the court of first instance).

This case is of great significance and enlightenment in China. When it is necessary to collect and use personal data, especially biometric data, data controllers processing activities.

SUGGESTIONS

Considering the current development and application of facial recognition technology and the regulatory tendency, facial recognition will undoubtedly be one of the focuses of personal data supervision in the future. Therefore, it is suggested for enterprises to fulfill their obligations of Multi-Level Protection Scheme (pursuant to the *Cyber Security Law*, the relevant national standards on personal data and other requirements).

For instance, companies should establish appropriate security technical measures and security management requirements, strict internal control and internal audit mechanisms, and improve the internal personal data protection system (customize their own applicable privacy policies, provide users with the right to choose, modify, delete, etc.).

In terms of external cooperation, when there is personal data transmission (especially personal sensitive data/biometric personal data), we suggest enterprises to require the partners to undertake the obligation of data protection, to sign relevant agreements and to evaluate the data security capability of the partners.

For any additional information please contact:

ZHANG Beibe
Associate- Shanghai Office
beibeiZHANG@dsavocats.com

Isabelle DOYON
Lawyer- Shanghai Office
doyon@dsavocats.com

The Newsletter is provided for general informational purposes only. Any information contained in this should not be construed as legal advice and is not intended to be a substitute for legal counsel on any subject.