

Translation



The following regulation defines the acceptable use of facial recognition technology in China. Its provisions to protect facial data privacy include stipulations that such data must remain on the original collecting device and not be transmitted over the internet, and that individuals must have another identity verification option besides facial recognition to log into apps and websites. The regulation includes a loophole that allows apparently unrestricted use of facial recognition technology for R&D and AI model training.

Title

Measures for the Security Management of Facial Recognition Technology Applications
人脸识别技术应用安全管理办法

Authors

Cyberspace Administration of China (CAC; 国家互联网信息办公室; 国家网信办) and Ministry of Public Security (公安部)

Source

CAC website. The Measures are dated March 13, 2025 and were uploaded to the website on March 21, 2025.

The Chinese source text is available online at:

https://www.cac.gov.cn/2025-03/21/c_1744174262156096.htm

An archived version of the Chinese source text is available online at: <https://perma.cc/RKF7-GL2Q>

Translation Date

April 1, 2025

Translator

Etcetera Language Group, Inc.

Editor

Ben Murphy, CSET Translation Manager

Measures for the Security Management of Facial Recognition Technology Applications

Cyberspace Administration of China

Ministry of Public Security

Order No. 19

The *Measures for the Security Management of Facial Recognition Technology Applications* were reviewed and adopted at the 23rd executive meeting of the Cyberspace Administration of China (CAC) on September 30, 2024 and approved by the Ministry of Public Security. The Measures are hereby promulgated and shall take

effect on June 1, 2025.

Director of the Cyberspace Administration of China Zhuang Rongwen (庄荣文)

Minister of Public Security Wang Xiaohong (王小洪)

March 13, 2025

Measures for the Security Management of Facial Recognition Technology Applications

Article 1 These Measures are formulated to regulate the use of facial recognition technology for processing facial information and to protect personal information rights and interests, in accordance with the *Cybersecurity Law of the People's Republic of China*,¹ the *Data Security Law of the People's Republic of China*,² the *Personal Information Protection Law of the People's Republic of China*,³ the *Regulations on Network Data Security Management* (网络数据安全条例), and other laws and administrative regulations.

Article 2 These Measures apply to activities using facial recognition technology to process facial information within the People's Republic of China (PRC).⁴

These Measures do not apply to the use of facial recognition technology to process facial information for research and development or algorithm training purposes within the PRC.

Article 3 Activities using facial recognition technology to process facial information shall comply with laws and regulations, respect social morality and ethics, comply with business and professional ethics, be honest and trustworthy, fulfill obligations to protect personal information, and bear responsibility to society, and shall not jeopardize national security or the public interest, or harm the legitimate rights and interests of individuals.

¹ Translator's note: An English translation of the *Cybersecurity Law* is available online at: <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>.

² Translator's note: An English translation of the *Data Security Law* is available online at: <https://www.chinalawtranslate.com/en/datasecuritylaw/>.

³ Translator's note: An English translation of the *Personal Information Protection Law* is available online at: <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>.

⁴ Translator's note: The Chinese word 境内 jìngnèi, translated throughout as "within the PRC," literally means "inside the borders [of mainland China]." China considers Hong Kong, Macao, and Taiwan to be part of China but not to be "within the PRC."

Article 4 The use of facial recognition technology to process facial information shall have a specific purpose and sufficient necessity, adopt the method that minimizes the impact on the rights and interests of individuals, and implement strict protection measures.

Article 5 Before using facial recognition technology to process facial information, personal information processors shall, in a prominent manner and in clear, easy-to-understand language, truthfully, accurately, and fully inform individuals of the following:

- (1) The name and contact information of the personal information processor;
- (2) The purpose and method of processing facial information, and the retention period;
- (3) The necessity of processing said facial information and its potential impact on the rights and interests of individuals;
- (4) The methods and procedures for individuals to exercise their legal rights;
- (5) Other matters required by laws and administrative regulations.

If any of the above matters change, individuals must be notified of the updated content.

Where laws or administrative regulations stipulate that notification is not required, such provisions shall prevail.

Processing facial information of persons with disabilities or older adults must also comply with national regulations regarding accessible environments.

Article 6 Where facial information is processed based on individual consent, such consent must be obtained separately and voluntarily under fully informed circumstances. Where laws or administrative regulations stipulate that written consent must be obtained for the processing of facial information, such provisions shall prevail.

Where facial information is processed based on individual consent, the individual has the right to withdraw that consent. Personal information processors shall provide a convenient and fast means for withdrawing consent. An individual's withdrawal of consent does not affect the validity of personal information processing activities that were carried out based on the individual's consent prior to the withdrawal.

Article 7 Where facial information of a minor under the age of 14 is processed based on individual consent, consent must be obtained from the minor's parents or other guardians.

When using facial recognition technology to process the facial information of minors under the age of 14, personal information processors shall formulate dedicated processing rules for the storage, use, transfer, and disclosure of such information, and lawfully safeguard the personal information of minors.

Article 8 Unless otherwise provided by laws or administrative regulations, or unless separate individual consent has been obtained, facial information shall be stored within facial recognition devices and shall not be transmitted externally via the internet.

Unless otherwise provided by laws or administrative regulations, the retention period for facial information shall not exceed the minimum duration necessary to achieve the purpose of processing.

Article 9 Personal information processors that apply facial recognition technology to process facial information shall conduct a personal information protection impact assessment in advance and keep records of the processing activities. The personal information protection impact assessment shall primarily include the following:

- (1) Whether the purpose and method of processing facial information are lawful, legitimate, and necessary;
- (2) The impact on the rights and interests of individuals, and the effectiveness of measures to mitigate adverse effects;
- (3) The risks of facial information being leaked, tampered with, lost, damaged, or unlawfully acquired, sold, or used, and the potential harm that may result;
- (4) Whether the protection measures adopted are lawful, effective, and proportionate to the level of risk.

The personal information protection impact assessment report and the processing records shall be retained for at least three years. If there is a change in the purpose or method of processing facial information, or if a major security incident occurs, a new personal information protection impact assessment shall be conducted.

Article 10 Where other non-facial recognition technology methods exist that can achieve the same purpose or meet equivalent business requirements, facial recognition technology shall not be used as the sole means of identity verification. If an individual does not consent to identity verification through facial information, other reasonable, convenient, and fast alternatives shall be provided.

Where other national regulations provide otherwise regarding the use of facial

recognition technology for identity verification, such provisions shall prevail.

Article 11 When using facial recognition technology to verify personal identity or identify specific individuals, it is encouraged to prioritize the use of channels such as the National Population Basic Information Database (国家人口基础信息库) and National Network Identity Authentication Public Services (国家网络身份认证公共服务), in order to reduce the collection and storage of facial information and safeguard its security.

Article 12 No organization or individual shall mislead, defraud, or coerce individuals into accepting identity verification via facial recognition technology on the grounds of business processing or improving service quality.

Article 13 The installation of facial recognition equipment in public spaces must be necessary to maintain public security. The facial information collection area shall be lawfully and reasonably defined, and clear signage must be displayed.

No organization or individual shall install facial recognition equipment inside private areas of public places, such as hotel guest rooms, public baths, public changing rooms, or public restrooms.

Article 14 Systems applying facial recognition technology shall adopt measures such as data encryption, security audits, access controls, authorization management, intrusion detection, and intrusion prevention to protect facial information security. Where such systems involve graded protection (等级保护) of cybersecurity or critical information infrastructure, obligations relating to graded protection of cybersecurity and critical information infrastructure protection shall be fulfilled in accordance with relevant national regulations.

Article 15 When the volume of facial information stored through the application of facial recognition technology reaches 100,000 individuals, the personal information processor shall, within 30 business days from that date, complete filing procedures with the local cyberspace administration (网信部门) at the provincial level or above. The filing application shall include the following materials:

- (1) Basic information about the personal information processor;
- (2) The purpose and method of facial information processing;
- (3) The quantity of stored facial information and corresponding security protection measures;
- (4) Processing rules and operating procedures for facial information;
- (5) The personal information protection impact assessment report.

Where substantive changes occur in the filing information, the filing amendment procedures shall be completed within 30 business days from the date of the change. Upon termination of the application of facial recognition technology, the filing cancellation procedures shall be completed within 30 business days from the date of termination, and the facial information shall be processed in accordance with the law.

Article 16 Cyberspace administrations, in coordination with public security authorities and other departments responsible for personal information protection, shall establish and improve mechanisms for information sharing and notification, and shall jointly carry out related work.

Cyberspace administrations, public security authorities, and other departments responsible for personal information protection shall, in accordance with the law, conduct supervision and inspection of personal information processing activities involving facial recognition technology. Personal information processors shall cooperate in accordance with the law.

Article 17 Any organization or individual has the right to file complaints or reports with departments responsible for personal information protection regarding unlawful use of facial recognition technology to process facial information. Departments receiving such complaints or reports shall handle them promptly and in accordance with the law, and shall notify the complainant or whistleblower of the outcome.

Article 18 Violations of these Measures shall be handled in accordance with relevant laws and administrative regulations. Where a crime is constituted, criminal liability shall be pursued as provided by law.

Article 19 For the purposes of these Measures, the following terms are defined as follows:

(1) Personal information processor: An organization or individual that independently determines the purpose and method of personal information processing activities.

(2) Facial information: Biometric information related to the facial features of an identified or identifiable natural person, recorded electronically or by other means; does not include anonymized information.

(3) Facial recognition technology: Biometric feature recognition technology that uses facial information to distinguish an individual's identity.

(4) Facial recognition device: A terminal device that uses facial recognition technology to distinguish an individual's identity.

(5) Identity verification: A one-to-one comparison of collected facial information with stored facial information in an information system to confirm whether the two match and refer to the same individual.

(6) Identification of a specific individual: A “one-to-many” comparison of collected facial information with facial information stored within a specific scope in an information system, used to discover and identify an individual with a specific identity.

Article 20 These Measures shall come into force on June 1, 2025.