Navigating face recognition technology: A comparative study of regulatory and ethical challenges in China and the European Union

Ina VIRTOSU,
PhD in EU Law, University of Macau, SAR Macau, China
yb67199@connect.um.edu.mo, ivirtosu3@gmail.com

Chen LI,
PhD in Law, Southwest University of Science and Technology, Centre for Latin American and Caribbean Studies, Mianyang, China
yb77204@um.edu.mo

Abstract
Face recognition technology, while advancing rapidly, presents unique challenges in both China and the European Union (EU). This comparative study explores the distinct regulatory, ethical, and social obstacles each jurisdiction faces. In China, the widespread implementation of face recognition is facilitated by a supportive regulatory environment and a societal emphasis on security and surveillance. However, this has raised significant concerns regarding privacy, data security, and the potential for misuse by the authorities or private entities. In contrast, the EU's stringent data protection laws, particularly the General Data Protection Regulation (GDPR), impose rigorous constraints on the deployment of face recognition technologies. These regulations aim to safeguard individual privacy but also create hurdles for technological advancement and implementation. Furthermore, public skepticism and ethical considerations in the EU limit the adoption of face recognition. This paper highlights the dichotomy between China's rapid technological adoption with lesser regulatory constraints and the EU's cautious, privacy-centric approach, highlighting the need for a balanced framework that can navigate the ethical implications and privacy concerns while fostering technological innovation and addressing societal security needs in both regions.

Keywords: valid consent, GDPR, biometric data, bias issues, PIPL.

1. Introduction

Facial recognition technology (FRT) stands at the intersection of rapid technological advancement and profound ethical debate, particularly in its varied application across different global regions. This technology, which enables the identification and verification of individuals based on their facial features, offers potential benefits for security, efficiency, and convenience. However, it also raises significant concerns regarding privacy, data security, and civil liberties. The regulatory, ethical, and social challenges associated with FRT are pronounced, and they manifest differently in diverse geopolitical contexts. This article explores these challenges by comparing the approaches of China and the European Union (EU).

This article delves into the dichotomy between China's rapid, regulation-light deployment of FRT and the EU's stringent, privacy-focused regulatory environment. By examining the regulatory frameworks, societal attitudes, and ethical considerations in each region, this study aims to highlight the broader implications of these differing approaches. The comparison illuminates the need for a balanced framework that can navigate the ethical implications and privacy concerns of FRT, while also fostering technological innovation and addressing societal security needs.

Ultimately, this article seeks to contribute to the global dialogue on FRT by offering insights into how diverse regulatory landscapes shape the deployment and societal impact of this technology. It underscores the importance of developing balanced policies that harmonize the benefits of FRT with the imperatives of privacy, ethical standards, and social trust.

2. Definition of FRT in EU laws

According to Guidelines 05/2022, adopted by the European Data Protection Board (EDPB), facial recognition is considered a probabilistic technology that can automatically recognise and authenticate persons based on their facial features [1]. FRT belongs to the wider area of biometric technologies. Under Article 4(14) GDPR, biometric data is defined as "personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data". The fact that facial images also constitute personal data was confirmed by both, the ECtHR [2] and the TCJEU [3]. The ECtHR has also stated that a person's facial image constitutes one of the key attributes of his/her personality, as it reveals the person's unique characteristics and distinguishes one person from another. The right to the protection of person's facial image is the essential components of personal development [4].

Using FRTs implies collecting, comparing or storing facial images for identification and authentication purposes, for border control, searching for people on police watch lists or tracking someone's activities in public places. FRT verifies a person's identity by examining the specific qualities and features of their face, in other words, biometric data to identify and/or verify a person's identification against previously recorded information [5].The use of AI-powered FRTs deploy more elaborate technologies and algorithms, involving the collection, storage, and processing of biometric data, which is considered highly sensitive under the GDPR (Article 4(13), (14) and (15) and Article 9) [6], but also under Law Enforcement Directive (LED) (Article 3(13) and Article 10) [7].However, LED is a more specialized regulation compared to the GDPR, so-called lex specialis, and applies specifically when public authorities handle personal data for the purposes of preventing, investigating, detecting, or prosecuting criminal offenses (Recitals 11 and 12 LED, and Recital 19 GDPR).

FRT is also regulated by the recent approved Artificial Intelligence Act (AI Act) [8]. The AI Act is the first of its kind in the world and it applies to the development, deployment, and use of AI in the EU or when it will affect people in the EU. AI Act covers all types of AI across a broad range of sectors, with exceptions for AI systems used solely for military, national security, research and non-professional purposes [8]. The AI Act categorizes AI applications not exempted from its regulations based on the potential harm they may cause, which range from unacceptable to high, limited, and minimal risk, with an additional classification for general-purpose AI [8]. Any applications posing unacceptable risks are prohibited, except in cases with specified exemptions. The EU AI Act forbids specific applications that influence individuals' choices or take advantage of their weaknesses, systems that assess or categorize individuals based on their social conduct or personal characteristics, and systems that forecast an individual's likelihood of engaging in criminal

activity [8]. Additionally, Article 5 (2) includes banning the use of "real-time remote biometric identification systems", i.e. AI systems from harvesting facial images from the internet or surveillance footage, deducing emotions within workplace or educational settings, and classifying individuals based on their biometric information [8]. This appears to encompass many algorithmic video surveillance applications. However, the restriction can be circumvented if the use of such systems is not conducted in real-time. Nonetheless, certain exemptions are granted for law enforcement activities, such as searching for missing persons, the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences or preventing terrorist attacks. The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement shall be deployed only to confirm the identity of the specifically targeted individual, and it shall take into account the following elements: (a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm that would be caused if the system were not used; (b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences [8]. "Real-time" biometric identification systems, including FRSs, can only be deployed if strict safeguards are met, e.g. its use is limited in time and geographic scope and subject to specific prior judicial or administrative authorisation. Using such systems post-facto is considered a high-risk use case, requiring judicial authorisation being linked to a criminal offence.

High-risk applications are those anticipated to present substantial risks to health, safety, or the fundamental rights of individuals. This notably includes AI systems employed in healthcare, education, recruitment, critical infrastructure management, law enforcement, or the justice sector [8]. Such applications are obligated to adhere to standards regarding quality, transparency, human oversight, and safety. In certain instances, they may necessitate a "Fundamental Rights Impact Assessment" prior to deployment. Evaluation is required both before market placement and throughout the lifespan of these applications. Additionally, the roster of high-risk applications can be expanded progressively over time, without requiring amendments to the AI Act itself.

3. Data protection and privacy concerns related to FRT in the EU

Using FRTs raise serious issues related to the right to personal data protection guaranteed in Article 8 of the Charter of Fundamental Rights of the EU (CFR), as well as the right to private life under Article 7 of the Charter [9]. Particularly, the initial video recording, continuing storage of the material, and the comparison of footage with database information for identification (matching) all interfere with or limit this right. Any limitation on these basic rights must be clearly justified and proportionate according to Article 52(1) CFR. To protect these rights, data controllers (and indirectly manufacturers) should design their intended data processing activities in full compliance with data protection principles, adhering to "data protection by design and by default" as stipulated in Article 25 GDPR and Article 20 LED [10]. Following the main legal principles of data protection (Article 5 GDPR and Article 4 LED), the processing of facial images must be based on lawful basis, valid consent, transparency, purpose limitation, privacy impact assessment, data minimisation, data accuracy, storage limitation, accountability and security measures.

3.1. Lawful basis

According to Article 52(1) CFR, any restriction on fundamental rights and freedoms must be established by law and must respect the core of those rights and freedoms [9]. Such restrictions must adhere to the principle of proportionality, meaning they can only be imposed if they are necessary and genuinely serve objectives of general interest recognized by the EU, or if they protect the rights and freedoms of others. For the processing of data to be lawful, it must comply with specific legal bases outlined in Recital 35 LED and Recital 40 GDPR. Video surveillance can be legally justified under Article 6 GDPR or under national laws implementing Article 8 LED. However, if it involves processing special categories of data, the processor must also meet the stringent requirements of Article 9 GDPR or Article 10 LED.

3.2. Valid consent

Processing personal data is generally prohibited, unless it is expressly allowed by law, or the data subject has consented to the processing. While being one of the more well-known legal bases for processing personal data, consent is only one of six bases mentioned in Article 6(1) GDPR, among others such as contract, legal obligations, vital interests of the data subject, public interest and legitimate interest [6]. Valid consent is one of the most problematic aspects when it comes to the deployment of FRT.

Consent is defined in Article 4(11) GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" [6]. The basic requirements for a valid legal consent are defined in Article 7 and specified in recital 32 GDPR:

a) Voluntariness: Consent must be given voluntarily, without any form of coercion or undue pressure. Individuals should have a genuine choice and be able to refuse or withdraw consent without facing negative consequences. In situations where FRT is used by authorities, individuals may feel pressured to consent due to perceived or real power imbalances.

b) Explicitness: Under the GDPR, explicit (unambiguous) consent is required from individuals before their biometric data can be collected and processed for facial recognition purposes, which means it requires either a statement or a clear affirmative act. This ensures that individuals are fully informed about how their data will be used and have actively agreed to it. Consent cannot be implied and must always be given through an opt-in, a declaration or an active motion, so that there is no misunderstanding that the data subject has consented to the processing.

c) Informed and specific consent: For consent to be informed and specific, the data subject must be provided with clear and comprehensive information about the controller's identity, the purpose, scope, and potential implications of the data collection and use. This includes details on data storage, sharing, and security measures. Also, shall be notified about his or her right to withdraw consent anytime. Many individuals may not fully understand how FRT works, the data it collects, or the implications of its use. Without a clear understanding, consent cannot be truly informed [11].

Obtaining consent for facial recognition in public or semi-public spaces (like streets,

airports, or shopping centers) is particularly challenging. It is often impractical to inform every individual and obtain their explicit consent, raising significant privacy concerns. A case related to privacy concerns regarding FRT occurred in Germany. In 2019, a German court ruled against the use of FRT by a major property management company, Deutsche Wohnen, in a residential complex in Berlin [12]. The court found that the company's use of facial recognition violated the GDPR and the residents' right to privacy. The case stemmed from complaints filed by residents and privacy advocates who argued that the technology was being used without their consent and raised concerns about surveillance and data protection. The ruling set a precedent for the use of FRT in residential settings in Germany and emphasized the importance of respecting individuals' privacy rights when deploying such technologies.

3.3. Transparency

According to the transparency principle outlined in Article 5(1)(a) of the GDPR, it must be clear to individuals that their personal data is being collected, used, consulted, or otherwise processed, and to what extent this processing occurs (Recital 39 GDPR) [6]. Data subjects must be properly informed about the processing of their data, including through FRT. This information should be provided either when the personal data is collected or before consent is given. This principle does not, however, prevent competent authorities from conducting activities such as covert investigations or video surveillance (Recital 26 LED). Article 13(3) LED allows Member States to introduce exceptions to avoid hindering ongoing investigations or to protect public and national security [7]. Such exemptions can be crucial for law enforcement, as informing a suspect about the use of FRT might compromise their efforts. Given that these exceptions limit data subjects' ability to exercise their rights, they must be strongly justified.

For video surveillance/FRT driven by AI under the GDPR, the EDPB recommends a two-layered approach to meet transparency requirements. Key information should be provided through a warning sign so that individuals can recognize the surveillance before entering the monitored area. Additional details can be made available through other accessible means, such as posters or websites, clearly referenced on the initial warning [1].

A notable case related to privacy concerns and legal challenges regarding facial recognition technology occurred in France. In 2020, the French data protection authority, Commission Nationale de l'Informatique et des Libertés (CNIL), fined a major retailer, Carrefour, for violating the GDPR due to its use of FRT in some of its stores [13].The CNIL found that Carrefour had failed to obtain proper consent from customers and did not provide sufficient transparency regarding the use of facial recognition technology. This case highlighted the importance of complying with GDPR regulations and ensuring transparency and consent when implementing FRT in commercial settings in France and the wider EU.

3.5. Fairness

The EDBP stated in its guidelines that "fairness is an overarching principle which requires that personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected, or misleading to the data subject" [1]. However, some scholars consider this principle is somewhat ambiguous that can be applied in

situations where data processing might be legally permissible but still seems unfair in the specific context [14].

3.6. Purpose limitation

The principle of purpose limitation dictates that personal data may only be processed for a specifically defined, explicit, and legitimate purpose and it is reflected in Article 8(2) CFR, Article 5(1)(b) GDPR, and Article 4(1)(b) LED [6, 7, 9]. This principle mandates that personal data must be processed solely for specified purposes, which must be explicitly defined by law, allowing individuals to foresee the intended use of their data. These principles also apply to the processing of data via facial recognition technologies, prohibiting the unlimited retention of such data. In this context, the intended purpose must be clearly articulated so that the individual concerned can understand how their data will be used and adhere to a high threshold, primarily focused on combating terrorism, serious crimes, identify missing persons and victims of crime, including children, which is the established purpose limitation under EU law for law enforcement access to various large-scale EU databases. However, designing IT systems, including facial recognition systems, for purposes such as combating serious crimes, terrorism, improving public safety, and curbing irregular migration carries the risk of function creep, where personal data (facial images) may be used for unintended purposes [5]. Given the significant risk of "function creep" associated with FRT, related systems and processes should incorporate safeguards, such as a compartmentalised architecture, to prevent unauthorized use. Even if access falls within the scope of the legitimate purpose, the principles of proportionality and data security may further limit access conditions [15]. To prevent this, safeguards must be implemented to ensure that facial recognition technology is not unlawfully used to access large-scale EU databases, particularly when considering interoperability of these databases.

3.7. Privacy impact assessment

Article 35 GDPR requires from controllers a Data Protection Impact Assessments (DPIA) prior to the processing of personal data, when these activities is likely to result in a high risk to the rights and freedoms of natural persons [6]. For instance, a DPIA is required when data processing activities includes systematic and extensive profiling with significant effects, processing of special categories of data or criminal offense data on a large scale, large-scale monitoring of publicly accessible areas (CCTV).

A DPIA shall include several key elements: a) description of processing activities; b) assessment of necessity and proportionality; c) risk assessment (identify the risks to individuals' rights and freedoms, considering both the likelihood and severity of these risks); d) mitigation measures; e) consultation with stakeholders [6]. Specifically, while considering the deployment of FRTs in uncontrolled environments, law enforcement authorities will have to assess and explain in their assessment the strict necessity and proportionality of the deployment of these technologies; address the risk to different fundamental rights, including data protection, privacy freedom of expression, freedom of assembly, freedom of movement or antidiscrimination, depending on the potential uses in different places [6]. The impact assessment could be carried out either by entities themselves or by an independent monitoring body or by an auditor having relevant expertise to help find out, measure or map out impacts and risks over time.

3.8. Data minimisation, data accuracy and storage limitation

The principle of data minimisation, as outlined in Article 5(1)(c) GDPR and Article 4(1)(c) LED outlines that the amount of data collected should be limited to what is necessary for the intended purpose and should not be excessive. EDBP suggest that this principle also involves anonymising data where feasible [16]. Thus any video material not relevant to the purpose of the processing should always be removed or anonymized, for instance by blurring with no retroactive ability to recover the data before deployment [7]. The EDPS has observed that FRT systems may not always comply with the principle of data minimisation [1].

The principle of data accuracy, stipulated in Article 5(1)(d) GDPR and Article 4(1)(d) LED, requires that personal data be factually and temporally accurate, meaning that certain data must be kept up to date [6, 7]. Accuracy is assessed based on the purpose for which the data was collected. Minor errors may not affect overall accuracy, such as a single faulty data point in a large dataset. The EU Agency for Fundamental Rights notes that accuracy typically means correctness for each individual, though it can be interpreted more broadly [17]. The Council of Europe's guidelines on facial recognition stress the need to avoid mislabeling and to test systems to eliminate demographic disparities, thereby preventing unintended discrimination [10]. Data controllers must check the quality of images and biometric templates in watch-lists to prevent false matches. The Article 29 of Guidelines on Automated individual decision-making suggests that even inaccurate inferences from accurate data could violate the accuracy principle, implying that algorithms must be trained on representative datasets with minimal hidden biases [18].This aspect of the principle remains debatable and unresolved.

The principle of data retention (storage limitation) mandates in Article 5(1)(e) GDPR and Article 4(1)(e) LED that data should not be retained in an identifiable form longer than necessary for its intended purposes. Typically, 72 hours is sufficient to determine whether data needs to be retained longer, allowing for the deletion of unnecessary footage. If storage exceeds 72 hours, substantial justification for the purpose and necessity of the extended storage must be provided. Data may be kept longer for specific surveillance purposes. The EPDB advises that data extracted from digital images to create templates should not be excessive and should only contain necessary information, thus preventing further unnecessary processing [19, 20, 21]. Additionally, depending on the purpose, the raw data used to generate facial templates should be deleted once the template is created.

3.9. Data security and accountability

The principle of data security requires that data be processed securely, protecting personal data against unauthorized or unlawful processing, as well as accidental loss, destruction, or damage, through appropriate technical and organizational measures (Article 5(1)(f) GDPR and Article 4(1)(f) LED) [6, 7]. Articles 32 GDPR and 29 LED (indirectly) mandate that controllers and processors implement measures to prevent unauthorized disclosure or access to personal data. The EDPB advises that controllers must protect the system and data during storage, transmission, and processing [22]. Measures should include compartmentalizing data during transmission and storage, storing biometric templates and raw data on separate databases, encrypting biometric data, especially templates,

establishing a policy for encryption and key management, implementing fraud detection measures, associating an integrity code with the data, and prohibiting external access to biometric data [22]. These measures should adapt as technology advances. The Council of Europe also emphasizes the need to prevent technology-specific attacks, such as presentation and morphing attacks [10].

4. Concerns about violating fundamental rights and freedoms through indiscriminate use of FRT in public spaces

Mass surveillance and concerns for fundamental rights have been highlighted by many authors in relation to the widespread adoption of FRT [19, 20, 23]. The use of technology to process biometric data on a mass scale, whether for law enforcement, public authority, or commercial purposes, poses unique and serious threats to privacy and security. The Council of Europe defines mass surveillance as any monitoring that is not directed in a "targeted" manner at a specific individual [24]. Extending the use of these systems beyond their initially authorized and controlled purposes introduces potential risks over time. Such extensions might include using data from social networks or databases initially intended for different purposes, repurposing a database beyond its allowed scope, or adding new functionalities to an existing system. Critics argue that this gradual extension may be part of a deliberate strategy by proponents to first implement facial recognition in seemingly legitimate contexts and then progressively broaden its application [19, 20, 23]. The use of technology to process biometric data on a mass scale, whether for law enforce [19, 25]. This type of surveillance lacks sufficient transparency, leaving people unaware of what is happening, unable to provide informed consent, and without a genuine, free choice to opt in or out.

European Commission investigations indicate that wherever such a system operates, the movements of individuals in the reference database can be tracked [26]. Investigations by the European Commission indicate that the deployment of such systems allows for tracking the movements of individuals within the reference database, significantly impacting personal data, privacy, autonomy, and dignity.[26] This practice raises new social concerns, such as the inability to move anonymously in public spaces and the pressure to conform, which could undermine free will. The Commission highlighted the necessity of an ex-ante mechanism to ensure compliance with requirements and obligations, ensuring that providers of AI systems, including FRT, implement measures to minimize risks to fundamental rights by design [27]. Without such measures, AI systems will not be allowed on the Union market. Additionally, ex post market surveillance and supervision by competent authorities are essential to investigate and sanction any violations of fundamental rights in a proportionate, effective, and dissuasive manner [6].

According to Article 52(1) of the Charter, any restrictions on fundamental rights and freedoms must be legally established and must not violate the core of those rights and freedoms. These restrictions must adhere to the following criteria:

1) *Provided by law*: This requirement ensures that any restriction on rights and freedoms has a clear legal basis and is subject to the rule of law. This legal foundation must be clear enough to inform citizens about the conditions and circumstances under which authorities can collect data and conduct secret surveillance. It must clearly outline the scope and manner in which public

authorities can exercise their discretion to ensure that individuals receive the minimum level of protection required by the rule of law in a democratic society. Since biometric data falls under the special categories of data listed in Article 10 of the LED, most FRT applications would require a dedicated law that clearly defines the application and conditions of its use, including specifying the types of crimes and, where applicable, the appropriate severity threshold.

2) *Respect the essence of rights and freedoms:* The essence of a fundamental right refers to its very core, which must always be respected, even when the right is restricted [28]. Human dignity must also be upheld in all circumstances. This means that even if a limitation is justified, it cannot be so extensive that it destroys the fundamental nature of the right or freedom [9]. Potential indicators of an infringement on this inviolable core include a) provisions that impose limitations regardless of an individual's conduct or specific circumstances; b) barriers that prevent or hinder access to the courts [29]; c) situations where the individual's circumstances are not considered before imposing a severe limitation [30].
3) *A legitimate aim* is a fundamental requirement for justifying any limitation on fundamental rights and freedoms. In the context of limitations under Article 52(1) CFR, legitimate aims typically include: a) public safety and security measures taken to protect national security, prevent crime, and maintain public order; b) efforts to protect public health and uphold societal moral standards; actions necessary to safeguard the rights and freedoms of other individuals; c) policies aimed at supporting the economic stability and well-being of the state; d) ensuring the proper functioning of democratic institutions and processes [9].
4) *Necessity and general interest:* According to established case law of the CJEU, any derogations and limitations concerning the protection of personal data must be applied only to the extent that they are strictly necessary [30, 31]. This also means that no less intrusive means are available to achieve the intended purpose and objectives of general interest recognized by the EU or to protect the rights and freedoms of others. These objectives include those stated in Article 3 TEU and other interests protected by specific provisions of the Treaties, such as establishing an area of freedom, security, and justice and preventing and combating crime. However, the deployment must be accompanied by strict safeguards to prevent abuse and ensure that it is used only for its intended purpose. Differential treatment can be justified if it aims to achieve a legitimate objective and the means used are necessary and proportionate [32].
5) *Principle of proportionality* is crucial when considering the deployment of FRT and shall correspond to the following criteria: a) appropriateness (the use of FRT must be suitable to achieve a legitimate aim, such as enhancing public security or preventing crime); b) necessity (there should be no less intrusive means available to achieve the same objective); c) balancing interests (the benefits of using FRT must outweigh the potential negative impact on individuals' rights and freedoms. This requires a careful and case-by-case assessment).

According to Amnesty International, the widespread and invasive nature of mass surveillance imposes constraints on everyone's engagement in social, public, and political activities [33]. According to a United Nations Human Rights Council report, using FRT to

identify individuals in the context of assemblies significantly undermines not only privacy, but also freedom of expression, and peaceful assembly [34]. It affects individuals' capacity to lead autonomous lives without altering their behaviors out of fear of constant surveillance and this situation hinders people from fully exercising their political and civil rights [34].

Religious freedoms are also at stake with the deployment of FRTs. Individuals practicing certain religions may be subject to heightened surveillance and discrimination based on their appearance or attire. Such surveillance can lead to a chilling effect, where people may feel compelled to alter their behavior or conceal their religious practices to avoid being targeted. This undermines the fundamental right to freely practice one's religion without fear of state interference or social discrimination.

The freedom of assembly and association is similarly jeopardized by the use of FRTs. Surveillance of public gatherings and protests can have a deterrent effect, discouraging individuals from participating in these activities due to fears of being identified and possibly facing repercussions [35].This is particularly concerning in contexts where people are advocating for political or social change. The deployment of biometric surveillance systems establishes a dynamic wherein the powerful observe while the powerless are subjected to observation [36]. This dynamic empowers disproportionately influential groups to reinforce their control over socially marginalized communities, including individuals living in poverty, experiencing social exclusion, people of color, and human rights activists [9].

5. Accuracy and bias issues

Article 21 CFR prohibits discrimination on various grounds, including sex, race, color, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership in a national minority, property, birth, disability, age, or sexual orientation. Additionally, Article 20 of the Charter states that everyone is equal before the law. Discrimination in data-supported algorithmic decision-making can arise for various reasons. Demographic bias in FRT refers to the tendency of these systems to perform differently across various demographic groups. This bias can manifest as varying levels of accuracy and error rates for different genders, ages, ethnicities, and other demographic categories. Biases, whether intentional or not, can be embedded during the design, testing, and implementation of facial recognition algorithms. Additionally, discrimination can occur based on how officers respond to matches produced by these algorithms. If an algorithm performs inconsistently across different groups, removing such bias through mathematical or programmatic means is often very challenging, and sometimes impossible.

One significant cause of discrimination is the quality of the data used to develop these algorithms and software [37]. If the datasets used to train facial recognition algorithms are not diverse, the resulting models may not perform well for underrepresented groups. For facial recognition software to be effective and accurate, it needs a large volume of facial images. More images generally lead to more accurate predictions. However, accuracy also depends on the quality of the images and having a representative set of faces from diverse groups. The design of the algorithm itself can introduce bias if it does not account for

demographic diversity. The way FRT is deployed and used can also contribute to bias, especially if it is not regularly monitored and adjusted for fairness [26]. Data accuracy is crucial for ensuring reliable identification, both factually and temporally. This accuracy is particularly vital in FR systems, where any discrepancies can lead to significant errors. Inaccuracies in data can lead to false positives, where individuals are wrongly identified [38]. This can have serious consequences, potentially leading to mistaken identity and causing harm or inconvenience to innocent individuals. Similarly, inaccuracies in data can result in false negatives, where individuals are not recognized when they should be. This poses a threat to security and can undermine the effectiveness of facial recognition systems [38]. Ensuring data accuracy is key to minimizing these errors and maintaining the integrity of such systems.

The EU Fundamental Rights Agency's 2019 report indicates that certain demographic groups are more susceptible to misidentification by FRT [39]. These groups typically include:

a) *Ethnic minorities*: Studies have shown that facial recognition systems often have higher error rates for individuals from ethnic minority groups due to biases in the training data and algorithms.
b) *Women*: Research has indicated that facial recognition systems tend to have higher error rates for women compared to men.
c) *Elderly people*: Age can impact the accuracy of facial recognition, with elderly individuals often facing higher misidentification rates.
d) *Children:* As vulnerable individuals deserving of heightened protection, children are particularly at risk when these technologies are employed in law enforcement and border management. The primary issue stems from the lower accuracy rates of FRTs in detecting and recognizing the rapidly changing facial features of young people. This inaccuracy can lead to higher rates of misidentification, resulting in potential harm and undue scrutiny of children.

As result there are several types of demographic bias:

a) Ethnic and racial bias, when FRT systems often show higher error rates for people of color. For example, currently, facial images used to develop algorithms in the Western world often over-represent white men and under-represent women and individuals from other ethnic backgrounds. Consequently, facial recognition systems tend to perform well for white men but poorly for black women [39].
b) Gender bias: Many FRT systems have been found to perform better on male faces compared to female faces.
c) Age bias, when there are differences in accuracy based on age, with systems often performing less accurately on younger and older individuals compared to middle-aged individuals. Given the vulnerability of children, processing their biometric data, including facial images, must undergo a stricter necessity and proportionality test compared to adults. This ensures that the use of such data is not only justified but also carefully limited to protect children's rights and well-being.
d) Bias can also arise based on factors like facial hair, glasses, or other accessories, which may be more common in some demographic groups than others.

Demographic bias in facial recognition technology is a significant concern that can lead to

unequal treatment and discrimination. By taking proactive steps to ensure diverse training data, detect and mitigate biases, and maintain transparency and accountability, developers and users of FRT can work towards more equitable and accurate systems.

6. Ethical and social implications of implementing FRTs in the EU

The public perception of FRT within the EU is multifaceted and complex. While some individuals acknowledge the potential benefits of facial recognition for enhancing security and streamlining various processes, there is a growing unease about its widespread deployment. This unease stems from concerns about privacy violations, data security, and the potential for misuse. People are increasingly aware of the implications of having their faces scanned and stored in databases without explicit consent, leading to fears of constant surveillance and loss of anonymity. Such concerns are particularly pronounced when the technology is used in public spaces, where individuals feel they have little control over their personal data.

A survey conducted across various EU countries provides insight into public perception regarding FRT [17].The data highlights levels of support, opposition, and neutrality towards the technology, as well as concerns related to privacy and discrimination.

Table 1. Public perception regarding implementation of FRTs

Country	Support FRT(%)	Oppose FRT(%)	Neutral FTR(%)	Concern Privacy(%)	Concern Discrimination (%)
France	45	35	20	70	55
Germany	50	30	20	68	60
Italy	48	33	19	72	58
Spain	47	34	19	69	57
Netherlands	52	28	20	65	53
Poland	49	32	19	67	56
Sweden	55	27	18	64	54

Source: EU FRA, Your rights matter: Data protection and privacy - Fundamental Rights Survey, 2020

Support for FRT varies across the EU, with Sweden showing the highest level of support at 55%, and highest opposition in France at 35%. Privacy concerns are significant, with Italy having the highest at 72%. Discrimination concerns are prominent, with Germany expressing the highest concern at 60%. The survey data indicates a complex and cautious public attitude towards facial recognition technology in the EU. While there is notable support for its potential benefits, significant opposition and neutrality reflect ongoing public debates about its implementation. Privacy and discrimination concerns are particularly prevalent, highlighting the need for robust regulatory frameworks and transparency measures to address these issues.

The ethical concerns surrounding the use of facial recognition technology primarily revolve around issues of surveillance and privacy. The idea that one's movements and activities can be continuously monitored and recorded raises significant ethical questions. There is a fear that this level of surveillance could lead to a society where people alter their behavior out of fear of being watched, thereby undermining personal freedoms and autonomy.

One of the critical ethical issues is the potential for abuse by those in power [17]. Facial recognition technology can be used to target and discriminate against specific groups, whether based on race, religion, or political beliefs [40]. The ability of authorities or private entities to track individuals without their knowledge or consent infringes on fundamental human rights, such as the right to privacy and freedom of expression. This concern is particularly relevant in the context of political protests or social movements, where surveillance could be used to intimidate or suppress dissent [41].

The ethical and privacy concerns significantly impact public trust and acceptance of facial recognition technology. Trust is eroded when people feel that their privacy is being invaded without adequate justification or oversight. The lack of transparency in how data is collected, stored, and used further exacerbates these concerns. For facial recognition technology to gain public acceptance, there must be clear and robust legal frameworks that regulate its use. These frameworks should ensure that the technology is used in a manner that is transparent, accountable, and respects individuals' rights.

For the technology to gain widespread acceptance, several measures need to be in place to address these concerns: a) implementing robust and comprehensive laws that clearly define when and how FRT can be used, ensuring that the use of such technology is always necessary, proportionate, and in line with human rights standards; b) transparency and accountability; c) data security; d) independent oversight; e) public engagement and education; f) ethical design and implementation, which includes addressing potential biases in the technology and ensuring that it does not disproportionately affect vulnerable groups.

7. Definition of FRT in Chinese laws

In China, FRT is the most extensively adopted form of AI, utilized across various sectors for diverse purposes such as identification and enhancing efficiency. The Chinese government acknowledges the efficiency benefits that facial recognition brings to both public and private sectors, and has prioritized its research, development, deployment, and commercialization [42]. Recognizing the role of FRT in enhancing public security, the Chinese government has widely implemented it as part of a broader national security framework, which also includes mechanisms like the social credit system [43]. Increasingly, state-owned enterprises in sectors such as telecommunications, banking, and transportation are recording citizens' facial data for their FRT systems. This technology is also prevalent in the private sector, where it is used for online payments, residential security, and hospital check-ins. The rapid advancement and extensive use of FRT have positioned China as a global leader in this field. Consequently, facial recognition has permeated nearly every aspect of daily life in China; for instance, it has been instrumental in managing the COVID-19 pandemic by enabling identity verification without physical contact.

FRT as defined under Chinese law generally refers to a biometric identification method that involves the automated recognition and analysis of individuals' facial features to verify identity. While there is no single comprehensive legal definition explicitly codified in a specific law, several regulations and guidelines provide context for how FRT is understood and regulated in China. Personal Information Protection Law of China (PIPL) The PIPL

categorizes facial data as sensitive personal information, which includes biometric characteristics. The law requires that processing such information must have a specific purpose and necessitate stringent protection measures [44]. Article 28 of PIPL stipulated personal information processors can only handle sensitive personal information if they have a specific purpose and sufficient necessity under protection by strict measures. Article 29 stressed that the processing of sensitive personal information needs the separate consent of the individual. Cybersecurity Law mandates the protection of personal data, including biometric information, emphasizing the need for consent and the secure handling of data to prevent misuse and breaches [45].

Thus, FRT in the context of Chinese law can be defined as "a biometric identification technology that uses automated processes to capture, analyse, and verify individuals' facial features for the purpose of identity verification, subject to regulations governing the processing of sensitive personal information, consent requirements, and data protection measures as stipulated by the PIPL and related cybersecurity regulations. This definition encompasses the core principles of FRT as regulated in China, emphasizing both its technical function and the legal framework governing its use.

8. Mandatory use of FRT and the issues of consent

FRT has raised significant privacy issues globally, and China is no exception. While some observers and the survey presented above suggest that Chinese culture may be more accepting of privacy infringements compared to Western cultures, and many Chinese people support FRT due to enhanced security and convenience, there have been extensive discussions about the rationale and appropriate extent of FRT deployment in the country [46]. China has been actively developing a regulatory framework for FRT since 2020. Despite aiming to significantly improve personal data protection, this framework faces growing risks and challenges in safeguarding citizens' data within the FRT landscape.

Undoubtably, FRT brings convenience to Chinese citizens in various scenarios, including cashless payments and bypassing security queues at metros, libraries, train stations, and airports. However, this convenience comes with challenges related to privacy and personal data protection, raising public concerns about the potential misuse of sensitive personal data [47]. The proliferation of FRT in numerous sectors has sparked growing concerns. Numerous media reports indicate that its application in the private sector is susceptible to issues such as lack of transparency and cybersecurity vulnerabilities, including data leaks. Regulatory concerns have also been raised, since a multi-agency task force report highlighted widespread privacy issues, noting that mobile applications using facial recognition often force users to provide facial data, lack clear rules for data collection, and fail to offer mechanisms for users to withdraw consent for the collection and use of their facial information [48].

On August 20, 2021, the National People's Congress passed the PIPL, marking the country's first comprehensive legislation on personal information protection set to take effect on November 1, 2021. Article 26 of the PIPL imposes restrictions on the use of FRT [44], stating that installation of devices for image collection and personal identity recognition in public places is permissible only if necessary to safeguard public security,

comply with relevant state regulations, and prominently display notices. The article also specifies that personal images and identification information collected can only be used to protect public security and must not be disclosed to others, except with explicit consent from individuals or as stipulated by laws and administrative regulations. Under the PIPL, biometric characteristics are categorized as sensitive information, requiring personal information processors to obtain consent from the data subjects and explain the necessity and potential impact of collecting such information.

FRT has become prominently utilized in the public sector, especially for law enforcement purposes such as identifying and tracking criminal suspects. Additionally, the government has designated facial recognition as a primary technology for identity verification in various regulations. It is strongly encouraged and often mandated for administrative tasks such as notarization, obtaining driver's licenses, and delivering social benefits to residents [49]. In April 2019, the General Administration of Customs authorized the use of facial recognition technology at Customs registration counters. Since September 2017, the Ministry of Justice has required parties seeking notarization to undergo identity verification using methods like facial recognition, cross-checking against the Ministry of Public Security's databases [50]. From January 2020, the Ministry of Public Security mandated that online traffic schools under the Traffic Management Department verify user identities using technical methods such as facial recognition [51]. Furthermore, during in-person traffic law education sessions organized by the Traffic Management Department, drivers' identities must also be verified through facial recognition technology [51]. Moreover, in February 2020, in response to monitoring and controlling COVID-19, Ant Financial introduced a QR code system that assigns users a color code indicating their health status [52]. Users obtain these codes by providing their name, national identity number, and registering with facial recognition. As it can be noticed these cases refers to public security and public health and all these regulations do not specify usage parameters or provide specific guidelines on how facial recognition technology should be deployed in public setting. Additionally, none of the rules issued address security measures aimed at protecting facial information.

With strong governmental backing, state-owned enterprises across various sectors have begun adopting facial recognition technology for identity verification purposes. For instance, the People's Bank of China, which has issued rules mandating FRT for verifying bank account identities since 2016. Banks are encouraged to utilize this technology to assist in reading, collecting, and verifying client information during account opening processes. The National Health Commission also promoted the use of FRT in pilot medical institutions starting from February 13, 2019, to strengthen the management. China Railway, where users are notified in the privacy policy that facial scans are required for logging into accounts using facial recognition. The Beijing Municipal Commission, which mandated the incorporation of FRT in public housing projects starting from January 2019 [53]. This is primarily aimed at enhancing security at entryways to prevent unauthorized access. And many other cases deployed by central and local authorities. These initiatives illustrate the extensive use of facial recognition technology by state-owned enterprises, primarily for streamlining identity verification processes across various administrative and service sectors.

Benefiting from government support and sometimes even mandates, numerous private companies are increasingly integrating facial recognition technology to improve operational efficiency. Across diverse industries, these companies are employing facial recognition primarily for managing user authentication processes. For instance, since December 1, 2019, mobile phone users in China are required to undergo facial recognition scans when registering new SIM cards. The Ministry of Industry and Information Technology mandated telecom companies to implement technical measures that compare the facial features of users with their identification cards [54]. Network access is only granted when the facial comparison matches the identification card information.

Using facial recognition in strictly personal settings can enhance efficiency, but it also poses challenges when private rights are disregarded. An example of this is the compulsory use of facial recognition without offering alternative solutions. In 2021, a property management company PMC "Wuye" was sued that it does not provide alternative methods for neighbourhood entrance verification [55]. The plantiff claimed that this PMC forces residents to use facial recognition and does not allow person to enter the neighbourhood if they refuse such technology [55]. The defendant argued that FRT is "the symbol of updated and reconstruction of old verification system" and it got consent with most residents only except the plantiff. From one side, facial recognition in Chinese society is considered to be a fashionable solution and become a key element evaluating the level of digitalization or "smartness" of neighbourhood management. Refusing FRT would be regarded as a "conservative or outdated" lifestyle. From the other side, the PMC do asked for consents from residents. However, according to the Judicial Interpretation of the Supreme Court [56] property owners shall be provided with alternative verification methods if a property management company insists on using FRT as the sole method for entry [56]. The parties reached an agreement that the PMC will provide entry method of using card key. From the Judicial Interpretation and litigation result, it can be found that the consent from the majority is not enough. Even if there is only single person who refuse to use FRT, the company must provide alternative solutions of the entrance verification.

The litigation dispute in question in the opinion of Court does not directly involve privacy violations or misuse of personal data, but rather concerns the compulsory use of personal information. Unlike cases where personal data is unlawfully used by third parties, mandatory facial recognition obtains user consent but may not be voluntary. While facial information collectors do not disclose any privacy, this still constitutes a breach of civil law because user consent may not be freely given. Article 1024 of Civil Code of China involves the protection on facial information from the perspective of civil law [57]. The Judicial Interpretation explained that the use of facial recognition without consent is a violation on right of personality [56], but kept silent on whether it is illegal in administrative cases and in public places. Article 4 of Judicial Interpretation rules that courts shall not support information processors' defenses of obtaining consents if: (1) the information processor refuses to provide products or services unless the natural person consents to the processing of facial information, except when the processing of facial information is necessary for the provision of products or services; (2) the information processor requires that the natural person should consent to the processing of facial information by means of

tie-in authorization; (3) the information processor forces directly or in a disguised form the natural person to consent to the processing of his/her facial information [56].

On August 2023, the Cyberspace Administration of China first disclosed the draft of "Provisions on the application of safety management of Face Recognition Technology (Trial)" (FRT Provisions) [58]. The FRT Provisions sets out that consent is compulsory requirement if information processors need to collect face images from users of applications. Article 5 FRT Provisions rules that the use of FRT to process face information shall obtain individual consent or written consent according to law, except for those who do not need to obtain personal consent according to laws and administrative regulations [58]. For the same arrangement, Article 13 rules that the separate or written consent of the parents or other guardians of the minors should be obtained if face information of minors under the age of 14 is processed [58]. Administrative regulation rules differently from judicial interpretation of civil law because it arranges exceptions for consent. If a civil litigation is triggered, the parties have to be both private ones and it is no doubt that there is no possibility for a private party to have right to use other's biometric information without consent. The PMC's behavior is also prohibited by the FRT Provisions: PMC shall not use face recognition technology to verify personal identity as the only way to enter and exit the property management area [58]. If individuals do not agree to use FR system verification, PMC shall provide other reasonable and convenient verification methods [58].

The Judicial Interpretation treat mandatory use "without consent" but it still makes an exception when FRT is necessary for realization of product or service functions [58]. The rules of FRT Provisions are stricter than those in Judicial Interpretation because it prohibits any use of FRT without consent for private purpose. It could be argued that continuing to use FRT in practice instead of discontinuing its use could serve as evidence of consent obtained, as supported by exceptions outlined in Judicial Interpretations, but Article 5 FRT Provisions even emphasized that written consent is necessary in some scenarios [58]. Therefore, consent should have a valid form.

Besides requirement on consent in facial information collection, the FRT Provisions also set other scenarios where consent is also mandatory. Article 7 rules that the installation of FRT in public places areas should satisfy the requirement of necessity for the maintaining public safety [58]. Entities operating such facilities and collecting facial images have the obligation to keep confidentiality of the obtained facial images and personal information, which does not allow relevant information to be illegally disclosed to the public or provided to third parties [58]. Even though consent to collect facial information is not required for public security purposes, the use of relevant information should be limited to such purposes. If relevant entities want to use collected facial information in other scenarios, they must obtain the consent of each individual [58], even though such entities may be bodies of the government. These provisions apply also in scenario when analysing other sensitive personal information via FRT, including race, ethnicity, religious belief, health status and social class, etc [58]. The exceptions to non-consent involve the maintenance of national or public security, and the protection of individuals' life, health, or property in emergencies. These two conditions differ in their requirements. While the FRT Provisions do not mandate an emergency element for national and public security scenarios, they do

require it for the protection of relevant rights. Therefore, consent from individuals is necessary if the situation is not urgent [58]. The FRT Provisions restrict not only the collection of facial information but also the handling of such information after collection. The provisions outlined in Article 12 emphasize the importance of balancing public safety with the protection of individual privacy rights in the context of using image acquisition and personal identification equipment in public places [58]. Here are some key points:

1. *Necessity and compliance*: The law mandates that the installation of such equipment should only be done when necessary for public safety. This is a reasonable measure to ensure that surveillance is not overused or implemented without justification. Moreover, the requirement to comply with national regulations and provide prominent notifications is crucial for transparency and public awareness.
2. *Confidentiality obligations:* The duty imposed on units to maintain the confidentiality of collected data underscores the importance of protecting personal information. By prohibiting illegal disclosure and external provision of data, the law aims to prevent misuse and unauthorized access, thereby safeguarding individuals' privacy.
3. *Purpose limitation:* Restricting the use of collected data exclusively to preserving public safety is a significant measure to prevent the abuse of surveillance technologies. This provision ensures that personal data is not exploited for other purposes, such as commercial gain or unwarranted monitoring.
4. *Consent requirement:* Allowing the use of personal images and identification information for other purposes only with the individual's specific consent is a critical aspect of data protection. It empowers individuals to have control over their personal information and ensures that their rights are respected.

These regulations reflect a thoughtful approach to integrating surveillance technologies into public spaces. They aim to harness the benefits of such technologies for public safety while imposing strict controls to protect privacy and prevent potential abuses. This balanced approach is essential in fostering public trust and ensuring that technological advancements do not come at the expense of fundamental privacy rights. Given the significant trust placed in governments using FRT, the exemption from consent collection for security reasons aligns with public concerns. Consent primarily becomes necessary when FRT is utilized for private purposes or by private entities, which underscores people’s apprehensions about the subsequent use of their facial information post-collection.

9. Abuse of facial information and issues of violation of civil rights

Misuse of Facial Recognition Technology (FRT) is anticipated to cause harm to individual rights such as personal identity, privacy, and other civil liberties. Typically, the misuse of FRT involves the absence of consent from individuals. In other words, any action taken without consent can be considered misuse of FRT, especially when it is mandated. In China, the misuse of FRT violates various regulations found in judicial interpretations of civil litigation, administrative laws and regulations, and criminal law.

9.1. Infringement of civil rights

In 2012 China's top legislative authority, the Standing Committee of the 11th People's Congress, expressed its commitment to safeguarding digital privacy. Plans were made to introduce legislation that included principles for data protection, such as restrictions on personal information collection and measures to ensure privacy protection [59]. The enactment of the 2020 PRC Civil Code marked a significant change in China's regulatory framework concerning the safeguarding of personal information, including biometric data. Prior to the Civil Code, regulations concerning personal data, including FRT, were fragmented, primarily addressed in laws related to cybercrime and cybersecurity breaches [57]. The Civil Code introduced a new chapter dedicated to privacy laws in China, recognizing personal information as a fundamental civil right. Article 1035 of the Civil Code sets forth general principles for data protection, including limitations on purposes and scope, as well as the requirement for informed consent from data subjects in the processing of personal information [57].

In the Judicial Interpretation of Supreme Court, abuse of FRT is consider to be "an action of infringing on the personality rights of a natural person [56]." It listed eight categories of abuse: (1) conducting facial verification, recognition, or analysis in business premises and public places by using FRT in violation of laws and regulations; (2) failing to disclose rules on the processing of facial information or failing to explicitly state the purposes, methods, and scope of such processing; (3) failing to obtain the separate consent; (4) not complying with the specified purposes, methods, and scope for processing facial information as stated by the information processor or agreed upon by all parties involved; (5) failing to take proper technical measures or other necessary measures for ensuring the security of facial information collected and stored, which results in leaks, distortion, or loss of facial information; (6) providing others with facial information in violation of the provisions of laws and administrative regulations or the agreement of both parties concerned; (7) processing facial information in violation of public order and good moral; (8) other circumstances where facial information is processed by violating the principles of lawfulness, legitimacy, and necessity [57].

9.2. Administrative law and regulations

According to the information disclosed by Institution of Judicial Case Study of the Supreme People's Court on August 18, 2021, the reporter found a total of 422 cases involving "face recognition" and "administrative penalty" in Weike Advanced Database (wkinfo) [60]. Among them, 29 cases are related to the protection of personal rights and interests in case of using FRTs and all occurred in the housing sales industry [60]. The report classifies into four categories:

Table 2 Types of abuse corresponding Judicial Interpretation

Type of Infringements:	Item in in the Judicial Interpretation
Not informing consumers of the collection of biometric data (face image)	Article 2(3)
Not clearly informing the purpose, method and scope of collection and use	Article 2(2)

Having informed the way to collect and use of biometric information (face image), but not specifying the true purpose and scope of their collection and use, nor having obtained the consent of consumers	Article 2(4)
Not specifying the purpose, method, and scope of collecting and using information to consumers with the consent of consumers	Article 2(2)

Source：Chu Xia, Analysis & interpretation on 400 administrative punishment cases of "face recognition"

Administrative authorities imposed fine on relevant parties in all 29 cases, according to Law on the Protection of Consumer Rights and Interests of China (LPCRI) [60]. Article 29 of LPCRI rules that operators shall follow the principles of legality, legitimacy, and necessity, specify the purpose, method and scope of collecting and using information, and obtain the consent of consumers [61]. When a business operator collects and uses consumer's personal information, it shall disclose its rules of collection and use. Such entity shall not collect and use information in violation of the provisions of laws and regulations and the agreements of both parties [61].

The analysis shows that different law rules concerning the use of FRT have similar norms. Even though Provisions on Facial Recognitions are still in the draft, other laws started to protect citizens from abusive use of FRT by commercial entities.

9.3. The application of criminal law for the abuse of FRTs

Besides civil liability and administrative fines, abuse or illegal obtaining of facial information may also receive criminal penalties. The Supreme Court of China disclosed Guiding Case no. 192 on Mr. Li Kaixiang's infringing citizens' personal information [62]. This case is a combination of criminal and civil litigation case for public interest purposes [62]. From June to September 2020, Li Kaixiang made a mobile phone "hacker software" with the function of illegally stealing the photos of the installer's album [62]. Through it, he stole a total of 1,751 photos from the installers' album, some of which containing 100 pieces of citizens' personal information including facial information [62]. On August 23, 2021, the People's Court of Fengxian District of Shanghai found that Li Kaixiang had committed the crime of infringing citizens' personal rights by stealing information and sentenced him to three years in prison but three years' probation, and a fine of 10,000 CNY [63]. The Fengxian court stated in its decision that "facial information" is recognized as citizens' personal information under the principle of law and order. Article 1034 of the Civil Code and the PIPL includes "facial information" in the category of sensitive information. Using hacker software to steal "facial information" is socially harmful and punishable by law. As sensitive information, "face information" is crucial for identifying individuals and has strong social attributes. It is easily misused or synthesized, potentially leading to privacy violations, reputation damage, theft, and fraud, posing significant social risks [62, 63].

The Supreme Court emphasized that face information generated or processed by FRT is highly recognizable [62]. It can be used to identify the identity of a specific natural person, or it can reflect the activities of a specific natural person alone or in combination with other information. Such information is regarded as the personal information under the criminal law. Article 5(4) of the Interpretation on Several Issues Concerning the Application of the Law in Criminal Cases of Infringement of Citizens' Personal Information may apply if a

person (1) collect or use facial information without the consent of the citizen himself, (2) does not have the legal reasons for the handling of personal information stipulated in the PIPL or the authorization of relevant departments; (3) steals or illegally obtains the above information by other means such as software programs [62].

Another similar case occurred when the first civil public interest litigation initiated by the Procuratorate regarding the protection of citizens' personal facial information was publicly adjudicated in Guangzhou [64]. The defendants collected high-definition ID card photos, ID card numbers and other personal sensitive information, then used the avatar in the photo to make AI videos and sell for money. The court ordered that the four defendants should immediately stop the infringement of citizens' personal information, pay compensation and damages, and apologize publicly [64].

10. Special regulation on FRT.

Article 6 FRT Provisions prohibits image acquisition and personal identification equipment to be installed in locations that might infringe on others' privacy, such as hotel rooms, public bathhouses, dressing rooms, and bathrooms [58]. The installation of FRT and personal identification equipment in public places must be done only when necessary to ensure public safety, adhere to applicable national regulations, and include clearly visible notifications [58]. Relevant entities have obligations to keep the obtained personal images and identification information confidentially and shall not be illegally disclosed or provided to the public [58]. Even though the use of FRT is for implementation of internal management, relevant entities should reasonably determine the image information collection area according to the actual needs, and take strict protection measures to prevent illegal access, copying, disclosure, external provision, dissemination of personal images, etc [58]. They should prevent the leakage, change, lost or illegally acquisition or use of personal information [58].

Security issues are also related to privacy. FRT Provisions give several requirements on security which aims to protect security:

Table 3. requirements on security in FRT Provisions

Article	Item	Content
17	Information preservation	Except under legal conditions or with individual consent, FRT users must not save original face images, pictures, or videos unless anonymized. Systems providing face recognition services must meet network security level protection above the third level and implement data encryption, security audits, access control, authorization management, and intrusion defenses. Critical information infrastructure must also comply with relevant security protection requirements.
18	Deletion or anonymization	The use of FRT to process face information shall try to avoid collecting face information that has nothing to do with the provision of services. If it cannot be avoided, it shall be deleted or anonymized.
19	Evaluation on security and risk	Users of face recognition technology must annually assess and mitigate security risks of image and identification equipment, adjust security strategies and confidence thresholds, and implement measures to protect against attacks, invasions, interference, and destruction.
20	Requirement on facilities	Image collection equipment and personal identification equipment listed in the catalogue of key network equipment and special products for network security

		in accordance with the relevant provisions of the State shall be sold or provided only after the qualified institutions have passed the certification or met the requirements in accordance with the mandatory requirements of relevant national standards.
21	Regular check	The network information department, together with the competent telecommunications department, the public security organ, the market supervision department and other relevant departments, shall strengthen the supervision and inspection of the use of face recognition technology according to their responsibilities, guide and urge users of face recognition technology to complete the filing procedures, find potential safety hazards in a timely manner and urge rectification within a timely limit.

Source: Provisions on the application of safety management of face recognition technology (Trial)

Besides substantive rules and ex-post regulation, FRT Provisions requires ex-ante compliance. Article 15 rules that FRT processors should conduct an impact assessment of personal information protection in advance and record the processing [58]. The impact assessment of personal information protection mainly includes the following: (1) whether it meets the provisions of laws, administrative regulations and the mandatory requirements of national standards, and whether it conforms to ethics; (2) whether the processing of face information has a specific purpose and sufficient necessity; (3) whether it is limited to the accuracy, accuracy and distance requirements necessary to achieve the purpose; (4) whether the protective measures taken are legal, effective and compatible with the degree of risk; (5) the risk of leakage, loss, destruction or illegal acquisition or illegal use of face information and possible harm; (6) the damage and impact that may be caused to the rights and interests of individuals, and whether the measures to reduce the adverse effects are effective [58].

The personal information protection impact assessment report shall be kept for at least three years. If the purpose and method of processing face information change, or a major security incident occurs, the user of face recognition technology shall re-evaluate the impact of personal information protection.

As for large scales of using FRT, extra evaluation process should be implemented. Article 16 of FRT Provisions rules that FRT processor who use FTR in public places or store more than 10,000 face information shall file with Cyberspace Administration at or above the municipal level within 30 working days [58]. The following materials shall be submitted for filing: (1) the basic situation of users of face recognition technology and their person in charge of personal information protection; (2) explanation of the necessity of handling face information; (3) the purpose, processing method and security protection measures of face information; (4) rules and operating procedures for the handling of face information; (5) personal information protection impact assessment report; (6) other materials that the network information department deems need to be provided.

FRT Provisions only provide general requirements, and detail things rely on different standards. Some of these standards are shown below:

Table 4. Standards related to FRT in China

Number	Type	Title	Promulgation	Validation
DB31/T 1467-2024	Shanghai Standard	Application Guide for Face Recognition Classification in Public Places	2024-04-02	2024-07-01
GB/T 42981-2023	National Standard	Information technology – Biometrics - Test methods for face recognition system	2023-09-07	2024-04-01
GA/T 1093-2023	Industrial Standard	Security prevention, face recognition application, entrance and exit control face recognition technical requirements	2023-07-28	2023-12-01
GB/T 41987-2022	National Standard	Public security - Face recognition applications - Test methods for presentation attack detection with fake face	2022-10-12	2023-05-01
GB/T 41819-2022	National Standard	Information security technology - Security requirements of face recognition data	2022-10-12	2023-05-01
GB/T 41772-2022	National Standard	Information technology - Biometrics— Technical requirements for face recognition system	2022-10-12	2023-05-01
YD/T 4087-2022	Industrial Standard	Mobile Intelligent Terminal Face Recognition Security Technical Requirements and Test Evaluation	2022-09-30	2023-01-01
SF/T 0106-2021	Industrial Standard	Inspection specifications for face recognition technology in portrait identification	2021-11-17	2021-11-17
GB/T 38671-2020	National Standard	Information security technology - Technical requirements for remote face recognition system	2020-04-28	2020-11-01
GB/T 35678-2017	National Standard	Public security - Face recognition application - Technical requirements for face images	2017-12-29	2018-07-01
SJ/T 11608-2016	Industrial Standard	General Specification for Face Recognition Equipment	2016-01-15	2016-06-01
GB/T 31488-2015	National Standard	Technical requirements for face identification of video surveillance in security systems	2015-05-15	2015-12-01

Source: National public service platform for standard information.

11. Ethical and social implications of implementing FRTs in China

In October 2020 Artificial Intelligence Ethics Research Group and the App Special Governance Working Group of the Nandu released the "Report on Face Recognition Application and Investigation on the Public (2020) (Nandu Report) [65]. In this report, the research groups mainly discussed the scenarios of using FRT, questions on public's acceptance on FRT and potential public concerns on FRT's risks. The Nandu Report listed ten types of scenarios using FRT, such as money transfer, opening and canceling accounts, real-name registration, unlocking and decrypting, face-changing applications, government affairs, traffic security inspection, access control attendance in campus/online education, public safety supervision [66]. The investigation shows that 94.07% of interviewees admitted that they used FRT in daily life [66]. Contrasting with this high percentage, the proportion of giving consent or having an agreement on using face information collection or privacy protection is much lower, only reaching 61.81% [66]. 18.59% of interviewees show that they did not see relevant agreements or consent polices [66]. The research

indicated that 61.81% of participants felt that their willingness to give consent for the use of FRT would vary depending on the specific scenario in which it is used. This suggests that compliance with consent protocols may be better in some situations but significantly worse in others. The research revealed that the use of FRT is higher in specific scenarios such as money transfers (67.17%), unlocking and decrypting devices (54.09%), traffic security inspections (49.63%), and real-name registrations (47.68%) [66]. This higher usage correlates with increased rates of obtaining consent and adherence to privacy policies. However, the potential risks of using FRT without proper consent and privacy protections are still prevalent. Big companies, including financial institutions, may conduct good due diligence process according to relevant rules on consent collection and privacy protection, but small developers of narrowly-used applications often may be very weak in such works. Even though FRT appears in many daily scenarios, it is not the most popular way for verification [66]. With a percentage of 32.98%, FRT ranks no.5 in the most popular method of verification, lower than fingerprint (55.7%), verification code on smartphones (50.66%), password (48.57%), and ID card (39.87%).[69] The primary concern arises when FRT is extensively and involuntarily implemented in everyday situations, either due to undesirable circumstances or mandatory requirements.

People concern on security issues caused by the use of FRT, with 63.64% of interviewees worry about leakage of facial information, ranking on the top of FRT risks. Others are personal tracking being recorded (54.4%), money loss (53.72%), fake news with manipulation of faces (49.59%), impersonation (37%) and reputation (13.91%) [66]. These risks are not unique for using FRT. Such risks may also appear when using other verification methods.

In contrast, interviewees support the use of FRT in public areas even though they suspect that it may bring risks on privacy since FRT in China is considered to be the guardian on public security. Up to 67.64% of interviewees can accept using FRT on detection of infringement of traffic rules and surveillance on urban roads and public transportation receives 64.77%. In contrast, only 39.22% of interviewees can accept that vendors use FRT to collect and analyse consumers' behaviours and preferences [66]. From this perspective, people welcome FRT in public scenarios but warry to be used for commercial purposes. Another evidence is that governments (74.06%), schools and universities (66.63%), SOEs (62.16%), and financial institutions (51.37%) received very high trustiness in using FRT [66]. Meanwhile, private companies only received 31.79% of trustiness [66].

Taking into account mandatory use of FRT in public by the government, it can also be concluded that people react very negatively on using FRT by private companies. Governments implement FRT to guarantee public security even though some personal rights may be sacrificed and limited, but in Chinse mindset this is for common good to all members in the society. If such mandating is implemented by private enterprises, there would be sufficient reason to suspect that face information would be misused or even abused, particularly for illegal purposes, which bring risks on individual security, privacy, and reputation, even though such risks are not unique in scenarios of using FRT.

12. Conclusions

The comparative study of face recognition technology (FRT) implementation in China and the European Union (EU) reveals stark contrasts driven by differing regulatory frameworks, ethical considerations, and societal values.

12.1. Differences in implementation

a) Regulatory environment and adoption:

- The EU has stringent data protection laws, primarily governed by GDPR, which imposes strict requirements on the collection, storage, and use of biometric data, including explicit consent from individuals, DPIAs, and strong security measures. These regulations are designed to safeguard individual privacy and ensure transparency and accountability in data processing. The strict regulatory framework and high public skepticism result in more cautious and limited adoption of FRT. There are significant legal and ethical hurdles that organizations must navigate to implement FRT.
- China has a more permissive regulatory environment regarding the use of facial recognition technology. The regulations are less stringent compared to the GDPR, allowing for broader deployment of the technology in various sectors, including public surveillance, without the same level of consent and transparency requirements. There are few legal restrictions on the collection and use of biometric data, giving authorities broad leeway to deploy FRT without significant oversight or accountability.

b) Purpose and usage:

- Facial recognition technology in the EU is often used in law enforcement, controlled settings such as airports, banks, and retail for purposes like security, identity verification, and customer service. There are significant restrictions on its use in public surveillance and law enforcement due to privacy concerns.
- In China, facial recognition technology is widely used for law enforcement, public surveillance, not only in in controlled settings, but also social credit systems. The government employs this technology extensively for monitoring, ensuring security, and maintaining social order.

c) Public perception and acceptance:

- There is significant public concern and debate about the use of facial recognition technology in the EU, driven by privacy advocates and civil rights organizations. The general public tends to be wary of extensive surveillance and the potential for misuse of biometric data.
- Public acceptance of facial recognition technology is higher in China, partly due to the government's narrative on the benefits of enhanced security and social order. The population is more accustomed to state surveillance and the use of technology for monitoring purposes.

d) Technological development and innovation:

- The EU's cautious, privacy-centric approach highlights the challenges of balancing technological innovation with robust privacy protections and ethical considerations. Innovation in facial recognition technology in the EU is influenced by strict regulatory requirements, which can slow down rapid deployment but ensure privacy and ethical considerations. European companies often focus on developing privacy-preserving technologies.
- China is a global leader in the rapid development and deployment of facial recognition technology, but at the cost of significant privacy and ethical concerns. Chinese companies benefit from a supportive regulatory environment and significant government investment, allowing for faster innovation and widespread implementation.

12.2. Similarities in implementation

a) Security applications:

- Both the EU and China use facial recognition technology for security purposes, such as access control in secure facilities, identity verification at airports, and enhancing public safety in crowded places.

b) Commercial use:

- In both regions, businesses are leveraging facial recognition technology for customer service improvements, personalized marketing, and efficient transaction processing. Retail stores, banks, and hospitality sectors are common adopters.

c) Technological capabilities:

- Both the EU and China have advanced technological capabilities in facial recognition. Companies in both regions are developing sophisticated algorithms and hardware to improve accuracy, speed, and reliability of facial recognition systems.

d) Ethical and privacy debates:

- Despite regulatory differences, there are ongoing ethical and privacy debates in both the EU and China regarding the use of facial recognition technology. Concerns about data security, potential misuse, and impacts on civil liberties are prevalent in discussions in both regions.

e) Need for a balanced framework:

- *Ethical and privacy safeguards:* Both regions need to find a balanced framework that addresses ethical implications and privacy concerns while fostering technological innovation. Such a framework should ensure that FRT is deployed in a manner that respects individual rights and societal values.
- *Regulatory harmonization:* There is a need for regulatory harmonization that can provide clear guidelines for the ethical use of FRT. This includes establishing international standards and best practices that protect privacy and prevent misuse while enabling technological advancement.

In conclusion, in China, the implementation of FRT is characterized by largely supportive regulatory environment that facilitates its widespread use into various aspects of public life,

including law enforcement, public surveillance, and even everyday commercial transactions. This broad adoption reflects a regulatory framework that prioritizes public safety over individual privacy. While this approach has enabled rapid technological deployment and enhanced security measures, it has also sparked significant ethical concerns. Issues such as privacy concerns, data security risks, and the potential for misuse of FRT highlight the dark side of unchecked technological growth.

In stark contrast, the EU's approach to FRT is governed by stringent data protection laws, reflecting a strong commitment to protecting individual privacy and data security. This regulatory framework ensures that technological advancements do not compromise fundamental rights, resulting in a more cautious adoption of FRT. Public skepticism and ethical concerns further constrain the deployment of FRT in the EU, where there is significant public and governmental scrutiny over its potential impacts on privacy and civil liberties. This cautious approach underscores the EU's prioritization of privacy and ethical considerations over rapid technological adoption.

References

[1] European Data Protection Board, "Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement," 2023.

[2] ECtHR, "Szabó and Vissy v. Hungary," no. 37138/14, 2016.

[3] CJEU, "M. Schwarz v. Stadt Bochum," no. C-291/12, 2013.

[4] ECtH8R, "Guide on Article 8 of The European Convention on Human Rights, Right to Respect for Private and Family Life," *Home and Correspondence*, 2019.

[5] M. Tambiama and M. Hendrik, "Regulating Facial Recognition in the EU," 2021. [Online].

[6] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119".

[7] "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities".

[8] Corrigendum, "Artificial Intelligence Act," *Interinstitutional file: 2021/0106 (COD)*, 2024.

[9] "Charter of Fundamental Rights of the European Union, 2000/C 364/01. Explanation on Article 52 - Scope and Interpretation of Rights and Principles," 2000. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT.

[10] Council of Europe, "Guidelines on facial recognition, Directorate General of Human Rights and Rule of Law, T-PD (2020)03rev4," 2021. [Online].

[11] European Data Protection Board, "Guidelines 05/2020 on Consent under Regulation 2016/679," 2020.

[12] Verwaltungsgericht Berlin , "Urteil des VG Berlin vom 27.06.2019 - VG 1 K 129.17," [Online]. Available: https://www.berlin.de/gerichte/verwaltungsgericht/.

[13] Commission Nationale de l'Informatique et des Libertés (CNIL), "Délibération SAN-2020-012," 2020. [Online]. Available: https://www.cnil.fr/fr/sanction-de-3-millions-deuros-pour-carrefour-france-et-800-000-euros-pour-carrefour-banque.

[14] P. Kramer, "'Artikel 5 DSGVO', in M. Eßer et al., Auernhammer DSGVO BDSG," 2020.

[15] European Union Agency for Fundamental Rights, "Under watchful eyes: biometrics, EU IT systems and fundamental rights, FRA," 2018.

[16] European Data Protection Board, "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default," 2020.

[17] EU Agency for Fundamental Rights, "Your rights matter: Data protection and privacy - Fundamental Rights Survey," 2020.

[18] European Commission, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679," 2018.

[19] S. Zuboff, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power," *Public Affairs,* 2019.

[20] B. Schneier, "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World," *W.W. Norton & Company,* 2015.

[21] V. Eubanks, "Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor," *St. Martin's Press,* 2018.

[22] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices," 2020.

[23] B. Wagner, "Ethics of AI and Robotics," *Springer,* 2020.

[24] Council of Europe, "Declaration on Mass Surveillance," 2015.

[25] K. Crawford, "Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence," *Yale University Press,* 2021.

[26] European Commission, "White Paper on Artificial Intelligence: A European approach to excellence and trust. COM (2020) 65 final," 2020.

[27] European Commission, "Impact assessment accompanying the Proposal for a Regulation of the European Parliament of the Council Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts. Commission Staff Working Document," 2021.

[28] CJEU C-279/09, "DEB Deutsche Energiehandels- und Beratungsgesellschaft mbH v Bundesrepublik Deutschland. Report of Case, 2010 I-13849," 2010.

[29] European Court of Justice, "Case C-362/14 Maximillian Schrems v Data Protection Commissioner," 2015.

[30] European Court of Justice, "Case C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications," Marine and Natural Resources and Others, 2014.

[31] "Case C-473/12, Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others," 2013.

[32] CJEU, "C-356/12, Wolfgang Glatzel v. Freistaat Bayern," 2014.

[33] Amnesty International, Russia, "Intrusive facial recognition technology must not be used to crackdown on protests," 2020.

[34] Office of the High Commissioner for Human Rights , "The impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests. A/HRC/44/24," 2020.

[35] D. Harwell and C. Timberg, "As Protests Spread Across the U.S., Facial Recognition and Surveillance Technology Comes Under Scrutiny," *The Washington Post,* 2020.

[36] E. Jakubowska and N. Naranjo, "Ban biometric mass surveillance," *EDRi,* 2020.

[37] EU Fundamental Rights Agency, "Data quality and artificial intelligence- mitigating bias and error to protect fundamental rights," *Publications Office,* 2019.

[38] Commission Nationale de l'Informatique et des Libertés (CNIL), "Facial Recognition: For a Debate Framed by the Law," 2019.

[39] EU Fundamental Rights Agency, "Fundamental Rights Report 2019," Luxembourg: Publications Office of the EU, 2019.

[40] J. Buolamwini and G. Timnit, "Gender shades: Intersectional Accuracy Disparities in Commercial Gender Classification," in *Proceedings of Machine Learning Research*, 2018.

[41] A. M. Bedoya, "The Color of Surveillance," *Georgetown Law Technology Review,* no. 4(2), pp. 109-142, 2020.

[42] Ministry of Industry and Information Technology of China, "Three-Year Action Plan to Develop a New Generation of the Artificial Intelligence Industry," 2017.

[43] J. A. Lee and P. Zhou. , "FRT Regulation in China," in *The Cambridge Handbook of Facial Recognition in the Modern State. Cambridge Law Handbooks,* Cambridge University Press, 2024.

[44] "Personal Information Protection Law of the People's Republic of China," 2021.

[45] "Cyber Security Law of the People's Republic of China," 2016.

[46] D. Ren, "AI, Machine Learning Tech Promises US$6000 Billion Annually for China Economy as It Pervades Industries, Says Mckinsey," 2022. [Online]. Available: www.scmp.com/business/banking-finance/article/3186409/ai-machine-learning-tech-promises-us600-billion-annually.

[47] T. G. Brown and a. et, "Public Debate on Facial Recognition Technologies in China," 2021. [Online]. Available: https://mit-serc.pubpub.org/pub/public-debate-on-facial-recognition-technologies-in-china/release/1.

[48] Cyberspace Administration of China, "Without the right of choice or the right to be informed, can facial recognition be trusted?," 2020.

[49] Y. Luo and R. Guo, "Facial recognition in China: Current Status, Comparative Approach and The Road Ahead, Penn Carey Law: Legal Scholarship Repository," 2022.

[50] Ministry of Justice of China, "Notice of the Office of the Ministry of Justice on Practical Guidance for Notarization," 2017.

[51] Ministry of Public Security of China, "Rules on Accepting Traffic Safety Education to Reduce Illegal Traffic Behavior (Trial)," 2020.

[52] M. H. Hu, "Beijing Rolls Out Colour-Coded QR System for Coronavirus Tracking Despite Concerns Over Privacy, Inaccurate Ratings," *South China Morning Post,* 2020.

[53] Beijing Commission of Housing and Urban-Rural Construction, "Notice on Further Strengthening of Supervision and Administration of Subletting and Leasing Public Rental Housing, Beijing Construction Regulation," no. 23, 2018.

[54] SOHU TECH, "China's Ministry of Industry and Information Technology's new implementing regulation. Beginning from December. 1, Application for Cards Requires 'Facial Recognition," 2019.

[55] R. S. Du and C. Y. Wan, "Suzhou court closed the first case of the latest judicial interpretation applicable to face recognition: Don't you want to enter the community without brushing your face? Court: Don't force it!," 2021.

[56] Supreme People's Court of China, "Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Civil Cases Relating to Processing of Personal Information by Using the Facial Recognition Technology, Interpretation No 15 [2021]," 2021.

[57] "Civil Code of the People's Republic of China," 2020.

[58] Cyberspace Administration of China, "Notice on the Provisions on the Safety Management of the Application of Face Recognition Technology (Trial) (Draft for Comments)," 2023.

[59] "Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks, issued by the Standing Committee of the National People's Congress," 2012.

[60] X. Chu, "Analysis & interpretation on 400+ administrative punishment cases of "face recognition"," *Institution of Judicial Case Study of the Supreme People's Court,* 2021.

[61] "Law of the People's Republic of China on the Protection of Consumer Rights and Interests," 2013.

[62] The Supreme Court of China, "Guiding Case No. 192: Li Kaixiang's Criminal Incidental Civil Public Interest Litigation Case for Infringing Citizens' Personal Information," 2022.

[63] "Criminal Judgment No. 828 (2021)," Shanghai, 2021.

[64] Y. Y. Zhong and et al, "Guangdong's first civil public interest lawsuit involving face recognition and personal information protection was sentenced", Jiancha Daily, Supreme People's Procuratorate (SPP) of the People's Republic of China," 2022.

[65] L. L. Fu, "Face Recognition Application Public Research Report (2020), Science and Technology Daily," 2020.

[66] "Artificial Intelligence Ethics Research Group and the App Special Governance Working Group of the Nandu (Southern Metropolis Daily), Report on Face Recognition Application and Investigation on the Public (2020)," 2020.

[67] EU Fundamental Rights Agency, "Data quality and artificial intelligence- mitigating bias and error to protect fundamental rights," *Publications Office*, 2019.