Dean&Francis
ISSN 2959-6149

# How and why is the use of biometric technology developing in China and how is this development affecting privacy in contemporary Chinese society?

**Ziqian Yang**

**Abstract:**

The dissertation investigates the evolution and repercussions of biometric technologies in current-day China, primarily on privacy and human rights. Using interviews and secondary literature review, it investigates the extent to which facial, fingerprint, and iris recognition have become more embedded in everyday life, government, and commerce. While these technologies enhance access, efficiency, and security in the daily lives of people, they also pose a risk to privacy and the use of data for unethical purposes. The dissertation compares Chinese privacy laws, especially the Personal Information Protection Law (PIPL), with laws in the EU, such as the GDPR, to show that governmental laws and regulations provide little actionable legal recourse. Finally, the dissertation makes the case for stronger laws and a need for greater public awareness of these increasing gaps in legal protection. The dissertation frames the rapid expansion of biometric technologies in its context and makes the case for a careful balance of the advancement of technologies and the rights of citizens to protect their privacy.

**Keywords:** Biometric technology, privacy, China, human rights, data protection

## 1. Introduction

In recent years, there has been globally significant growth and development in biometric technology and its applications and usage. This growing investment and application and biometric technology is happening not only in the private sector by companies and businesses but also by the governments. In China to a much greater extent than in other jurisdictions. During the COVID pandemic and post COVID era, biometric technologies, such as fingerprint recognition, facial recognition, and iris recognition usage have accelerated at an alarming rate with limited legal or regulatory oversight, and with limited regard to human rights and the right to privacy. These biometric technologies have been used extensively and

ISSN 2959-6149

are becoming increasingly embedded in Chinese society, culture, and the economy.

The Rolling out of facial recognition, technology software, and fingerprint ID during COVID-19 proceeded at an unprecedented, rate Facilitating a very high level of surveillance of Chinese people.

Advanced face-matching technology controlled by Artificial intelligence, for example, being part of the biometric technology is so advanced now that it negates the use of masks to hide identity. Thus, this has been used to surveil people making anonymity in a public place virtually impossible (Biometrics Institute, 2020). According to estimates, in 2023, after COVID, Shanghai had the highest number of surveillance cameras among China's cities; with over 5,000 cameras per square mile. The city of Shanghai was only preceded by Wuhan and Shenzhen regarding the density of CCTV cameras (Slotta, 2024).

The wide usage of surveillance cameras with Facial recognition, technology, and software in China has raised people's concerns about their privacy and safety. This is also a live issue of discussion and debate in both America and Europe. In the UK, for example, cases have been brought before the courts to challenge the police use of facial recognition in public places known as AFR - Automatic facial recognition. The high court ruled in 2020 that the application of AFR breached the right to privacy under Article 8 of the European Convention on Human Rights (Sabbagh, 2020). Moreover, companies are gathering people's information, thus raising new concerns about privacy and "information leakage".

It is important to put this Critical topic of the use of biometric technologies into the context of how it is being used in China and how it impacts upon human rights and privacy.

In an increasingly digital world, biometric technology is becoming present in more areas of society and economy and implications of this technology for privacy are significant. In Europe, Article 8 of the European convention on human rights and article 12 of The Universal declaration of human rights both provide that privacy is a fundamental human, right. article 8 Defines privacy, as the right to respect of a private life, home and correspondence. In China, a lot of families also raise awareness on their privacy safety and considering how to protect their privacy under biometric technologies' wide use.

This dissertation aims to explore the relationship between biometric technology, and privacy security. It seeks to question the role of law in this relationship, such as regulating the usage of biometric technology to protect people's privacy and data security.

Additionally, this study will attempt to research the sentiment of contemporary society in China toward biometric technologies, their usage in daily life. It will also explore the need for regulation to protect people's right to privacy against this background.

## 2. Literature Review

### 2.1 The Use of Biometric Technologies in China and abroad

Biometric technologies are based on biometrics characteristics. Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic (Vacca, 2007). Nowadays, these technologies have become part of people's lives with a wide range of applications shown in Table 1.

**Table 1. Applications of three biometric technologies (Unar, et. al, 2014)**

| Biometric technology | Applications |
|---|---|
| Fingerprint recognition | Border control, forensics, criminal identification, access control, computer logins, e-commerce, welfare disbursements, missing children identification, id cards, passports, user authentication on mobile devices, time and attendance monitoring systems |
| Facial recognition | Border control, forensics, criminal identification, access control, computer logins, e-commerce, welfare disbursements, missing children identification, id cards, passports, video surveillance, crowd monitoring |
| Iris recognition | Border control, criminal identification, access control, computer logins, ecommerce, welfare disbursements, missing children identification, id-cards, passports, time and attendance monitoring systems |

A comparison of three main biometric recognition techniques and their traits is presented in Table 2 below.

**Table 2. Comparison of selected biometric technologies, adapted from (Dass, 2013)**

| Biometric trait | UVSL | DSTC | PRMN | CLTB | PRFM | ACPT | CRVN |
|---|---|---|---|---|---|---|---|
| Face | H | L | M | H | L | M | H |
| Iris | H | H | H | M | H | L | L |
| Fingerprint | M | H | H | M | H | M | M |

H, high; M, medium; L, low, respectively; UVSL, universality; DSTC, distinctiveness; PRMN, permanence; CLTB, collectability; PRFM, performance; ACPT, acceptability; CRVN, circumvention

Facial recognition relies on the unique features of the human face, which have high universality, relatively low distinctiveness, medium permanence, high collectability, respectively low performance, medium acceptability, and high circumvention.

Iris recognition technology uses a video-based system that locates the eye and Iris, evaluates the degree of occlusion by eyelid and spectral reflection; determines the quality of image focus; and determines the center and boundary of the pupil and the limbus (outer edge of the iris) for processing (Williams, 1996). The iris trait shows high universality, high distinctiveness, high permanence, medium collectability, high performance, low acceptability than the other two traits, and low circumvention.

Fingerprint recognition, widely used in various fields, such as law enforcement and medicine, identifies people through the uniqueness of their fingerprints. It shows medium universality, high distinctiveness, high permanence, medium collectability, high performance, medium acceptability, and medium circumvention.

During the COVID-19 pandemic, the need for people to wear masks leading an increased use of biometric technologies in China. Additionally, biometric technologies are globally used in login of smartphones. As shown in Table 3, based on estimation, biometric technologies as a tool for smartphone logins are implemented in the world dramatically. There will be more than 1.3 billion devices having the capability of facial recognition in the year 2024 and for the 90% percent estimation, it will grow over 50% each year (Juniper Research, 2020). This increasing number directly shows the wide use of biometric technology use in smartphones. Specifically, as of December 2023, the adoption rate of mobile payment among mobile internet users in China was over 87.3 percent, representing a user base of 954 million (Slotta, 2024).

**Table 3. Estimated number of phones with biometric technologies (Pascu, 2020)**

| Biometric technology | Estimated number of smartphones with it by 2024 |
|---|---|
| Facial recognition | 90% of the total smartphones |
| Fingerprint recognition | Over 4.6 billion smartphones |

## 2.2 The Background of human rights

Human rights are rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion, or any other status; Human rights include the right to life and liberty, freedom from slavery and torture, freedom of opinion and expression, the right to work and education, and many more (United Nations). The right to privacy as part of human rights is a key aspect not only in China but also globally. A general definition of privacy is the right to be let alone, free from interference or intrusion (UCSD, 2024).

Tracing back the history, human's understanding of privacy has changed and improved over time. In Epictetus's philosophy, he maintained that he had an "existence", an inner "thing" (OLL). Epictetus, a Greek Stoic philosopher, believes that he has an inner feeling that is not subject to external coercion. He splits a person into internal and external under the discussion on privacy.

Other scholars have mentioned the importance of public view in defining privacy. Imagine participating in a big activity with a group of people, such as joining the National Association for the Advancement of Colored People or performing an act of public worship in a church or synagogue, a person may claim the right to be let alone when he acts publicly as when he acts privately (KoivTz, 1966). The essence here is the understanding of having own choices to not be forced to participate in any activities.

China's legislation (Article 1032 in Chapter IV of the Civil Code of the People's Republic of China) states that privacy is the undisturbed private life of a natural person and his private space, private activities, and private information that he does not want to be known to others. At present, there is no specific individual privacy protection act in China. The contents of protecting people's privacy

ISSN 2959-6149

are mainly included in the Constitution of the People's Republic of China and the Law of the People's Republic of China on Penalties for Administration of Public Security.

### 2.3 The law protecting people's right to privacy under the wide use of biometric technologies

Before examining a specific area, it is necessary to clarify the definition of law. Law is a rule, usually made up by government, that is used to order the way in which society behaves (Cambridge Dictionary, 2025).

In China, laws related to biometric technologies and people's privacy include the Personal Information Protection Law of the People's Republic of China (PIPL), the Civil Code of the People's Republic of China, and so on. The following literature review will mainly focus on explaining the PIPL.

Before introducing the PIPL, it is worth discussing the Social Credit System (SCS) in China. China's social credit system refers to a diverse network of initiatives aimed at enhancing the amount of 'trust' within Chinese society (Donnelly, 2024). The Social Credit System mainly rates people through many aspects, such as past aggression behavior record, credit in society, and so on.

The relationship between PIPL and SCS can be generalized as the following. PIPL is a critical component in the local and extraterritorial design of China's model of cross-border data access; SCS serves to internally consolidate data feeds and flows (Calzada, 2022).

Other countries in the world, for example, the United Kingdom, also have laws protecting people's right to privacy under the fast development of biometric technologies. In the Human Rights Act, it is clearly stated that people have the right to live their lives privately without government interference (Equality and Human Rights, 2021).

Specifically, to protect people's human rights under the wide usage of biometric technologies, United Kingdom has the General Data Protection Regulation (GDPR). GDPR clarifies the definition of important terms, for example personal data, principles relating to personal data, and so on. GDPR shows that 'personal data' means any information relating to an identified or identifiable natural person ('data subject') (GDPR, 2016).

Comparing the law about protecting the right to privacy under the use of biometric technologies in China and the United Kingdom, it is likely to find out that the UK has more specific laws about biometric technologies. Especially when focusing on criminal law protection, it is likely to find out the result. China's criminal law has not written citizens' personal biometric information into criminal law to provide strong protection.

## 3. Methodology

### 3.1 Overview

This dissertation focuses on two issues. First of all, the potential harm of using biometric technologies and how to supervise the use of these technologies. Second, how could biometric technologies be regulated by law to better protect people's human rights? This article will continue to analyze the advantages and disadvantages of fingerprint recognition, facial recognition, and iris recognition and feasible legislation combined with interviews results and secondary research results.

### 3.2 Secondary research

The second-hand literature of this dissertation mainly comes from Google Scholar, IEEE, and various research report websites, for instance, Biometric Institute. At the same time, the author has gotten some resources through China's news agencies, such as Guangzhou Daily.

Chinese legal provisions are from the official website or scholars' analysis. For the UK legal provisions are all obtained from official websites, such as the GDPR website, Equality and Human Rights website, and so on.

By searching keywords such as "biometric technologies", "facial recognition", "iris recognition", "fingerprint recognition", and "legislation" in the database of academic websites, the above secondary information was obtained.

### 3.3 Primary Research

This article adopts the method of interview, interviewing a total of a 2 people from different regions of China. These two people have different ages, identities, and experiences of using biometric technologies. Both of the interviewees have legislation-related background.

The first interviewee is an 11th grader, who is 17 years old and studying in high school. The interviewee has the pseudonym, Lucy. Lucy is interested in laws and has already participated in several Model United Nations conferences related to laws. Moreover, Lucy had once conducted research in natural law and planning to study law when stepping into university.

The interview II is with an adult, who is 49 years old now. This interviewee is given the pseudonym Jenny. Jennies had graduated from university and majored in law. After university, she had worked as a lawyer in China for 15 years.

A total of 10 questions were asked. These two different age-group people can reveal part of Chinese people,

especially those who have expertise in law, and current thoughts on the wide use of biometric technologies. Therefore, their answers can be used as a basis for the improvement in establishing the legislation supervision of biometric technologies.

# 4. Results and analysis

## 4.1 Advantages of biometric technologies

### 4.1.1 Convenience of biometric technologies

Convenience is one of biometric recognition technology, which can be also called biometric technologies, biggest advantage. Biometric technologies after installed on smartphones have make time use more efficiently. According to Lucy, biometric technologies, such as fingerprint recognition, iris recognition, and facial recognition, allow her to pass the login process quickly.

The following table is a comparison of the traditional common payment method in China with the newest facial recognition as a method of payment. Using facial recognition to finish payment only took 10-15 seconds which is faster than QR-code scanning or Apple pay or Android pay.

**Table 4. Comparison between traditional method of payment and facial recognition payment (Liu, 2020).**

| Payment Methods | Device Requirements | Software Requirements | Time Cost |
|---|---|---|---|
| Apple Pay or Android Pay | A phone that supports facial recognition | Credit/debit card preset in Apple Pay | Within 15s |
| QR-code Scanning | A smartphone with a camera | An Ali Pay/WeChat account and an associated bank account | 30s – 1min |
| Facial Recognition | None (well, a face) | An Ali Pay/WeChat account and an associated bank account | 10 – 15s<br>(For frequent users, it could be less than 10 seconds) |

Besides, when using biometric technologies in digital payment, according to Jennie, biometric technologies allow her to quickly complete the payment online. With the increasing popularity of mobile banking, facial recognition technology can be used to verify a customer's identity before providing access to their account (Mishra & Dash, 2023). This level of convenience is particularly appealing in retail environments, where quick and efficient transactions are essential (Maskey, 2024). However, whether this recognition method is used for surveillance purpose is becoming a question. Moreover, what is the data used for also is a significant privacy-related concern.

### 4.1.2 Effectiveness

Biometric technologies are effective. The biometrics systems are effective for human identification and authentication over various levels of implementation, such systems are difficult to forge and can be made secure by combining more than one biometric trait, that is multimodal biometric systems (Tiwari, et. al, 2015).

For example, in the financial and bank area, after the biometric technologies are implemented, customers will save more time. The new biometric authentication speeds up access to accounts by some 70% faster than the traditional mode of keying in the conventional 6-digit personal identification number (PIN) (Ho, 2015). With biometric technologies being implemented in the banking access system, people's time will be saved thus achieving the goal of effectiveness. Besides, from an education perspective, biometric technology is a necessary step to strengthen authentication and monitoring in the context of distance education (Arista, et. al, 2024).

### 4.1.3 Low cost

Most biometric technologies can be implemented at low cost, such as fingerprint recognition and facial recognition. Facial recognition is eased to use and a low cost of system implementation; fingerprint recognition with low requirement in power lowers the cost of implementing this technique (Alsaadi, 2015).

Biometric technology systems can be designed on their own, for example, fingerprint recognition equipment. The material used was VeroWhite, a rigid opaque photopolymer from a manufacturer called Stratasys, and was printed on a Stratasys Objet500, Connex3 3D printer; the cost of the printed part was less than five dollars (Costa-Abreu & Smith, 2017).

### 4.1.4 Security

Biometric technologies have fewer security concerns than traditional methods when people need to pay, because of people's non-copyable and unique biometric traits. Individuals perceive fingerprint biometrics with less security concern than credit card only or credit card + PIN payment authentication methods (Ogbanufe & Kim, 2017).

ISSN 2959-6149

Moreover, biometric technologies are more stable. The iris is a protected internal organ whose texture is stable and distinctive, even among identical twins (similar to fingerprints), and extremely difficult to surgically spoof (Jain & Kumar, 2012). Therefore, biometric technologies will be more stable than traditional methods.

Biometric technologies can be implemented in government system and help to achieve political equality. With the help of biometric technology, it has become possible for governments to minimize the occurrence of any fraud during any transactions or through the elections (Alenizi & Al-Karawi, 2022).

Moreover, using biometric technologies to identify criminals easily. A study result shows that the majority of the respondents agreed with the statement that the use of biometric fingerprint technologies has decreased the number of illegal entries for expellees who tried to re-enter the country to a high extent (mean=4.07) (Tangai, et.al, 2019). Using biometric technologies for identifying criminals is useful, but it raises another question that is using biometric technologies in law-enforcement process means that criminals can be tracked and monitored. This is another biometric related problem under the safety, as a benefit, biometric technologies that worth discussing in the society.

## 4.2 Disadvantages bring by using biometric technologies

### 4.2.1 Reliability

Biometric technologies by capturing the biometric characteristics of a person may make false judgments. There is a real example of facial recognition, as a type of identification powered by biometric technologies, failing to distinguish from identical twins. The machine using WeChat payment identifies the elder brother as the younger brother and deducts the younger brother's money. Wrong identification of similar people in society by facial recognition technology may create loss to people. Facial recognition systems being a typical type of technology have this problem, even though they may be trained and tested on thousands or even millions of faces (Metz, 2019).

In the case of reliability, if the technologies are protecting privacy properly, the reliability of this biometric technology will increase. Moreover, it is essential to avoid collecting too much data or use the personal information contained and collected for the use of biometric technologies improperly.

### 4.2.2 Privacy Leakage

Access to the database, which did not require a password, was shut down after an anonymous user advertised more than 23 terabytes (TB) of data for sale for 10 bitcoin – roughly $200,000 (Xiong, et. al, 2022). Approximately 1 billion people's data collected by the Shanghai police are stored in this database. The trove of data contains names, phone numbers, government ID numbers, and police reports (Newman, 2022). This event has raised severe concerns on the privacy safety and how to prevent information from privacy leakage.

In China, since biometric technologies have been widely used, almost every person's biometric data is being collected, and some people will use other's information illegally. In the past few years, selling and buying illegal identity cards in China have been happening. Five men in Guangzhou, China had bought related technology support online and then mastered the skills of changing a person's personal photo to a live video AI technology (Zhang, 2024). Even though, this case seems to be mainly related to the illegal use of AI technology, it still includes misuse of biometric technologies which is where the man got a different picture from a different person. Before the five offenders in the case started to use AI technology to create live videos, they needed to have different people's face photos, which are being provided by an intermediary agency. The intermediary agency acts like an information transfer center by receiving the AI mimic photos from individuals and then sending the new videos to companies to change the information in other apps by using these new AI-generated photos to pass the facial recognition system. The distinct process of embezzling others' information to create illegal profits leads people to question are their privacy is being protected. Governments and companies should increase supervision of the protection of biometric technologies related to personal information. People should also raise their awareness when giving a company consent to use their personal biometric traits.

## 4.3 Misuse and the ethics of using biometric technologies

As analyzed above, biometric technologies have brought several advantages along with several disadvantages as well.

Facial recognition is useful in identifying people's face. However, when raising people's attention to obey traffic regulations, facial recognition is being misused. The street establishes a LED screen and people who working pass by will be recorded and their face will show on this screen. Even though the purpose of this action is positive, it has unintentionally harmed people's privacy.

Facebook CEO Mark Zuckerberg admitting that Facebook's real goal was to manipulate and exploit its users (Washington Post, 2019). Biometric technologies have

been misused by these companies. This raises severe concerns about privacy leakage and the question of the ethics of using biometric technologies.

### 4.4 Biometric technologies during COVID-19

During the COVID-19 period in China, the use of biometric technologies in real life have increased dramatically. Surveillance cameras, the requirement of holding the QR code to show that you are healthy, and several other events that related in using biometric technologies.

On a grand scale, it (fever and temperature detection) is being delivered through CCTV infrastructure, surveillance cameras, infrared systems, and security checkpoints used in transportation and border control (Carlaw, 2020). When using these cameras and several biometric systems for detecting fever and temperature, harms people's right to privacy. By using these systems, people lose the opportunity to be "let alone".

Moreover, during the COVID era, it is also important to supervise the heartbeat rate. Some electrocardiogram (ECG) patches, such as iRhythm, and ZioXT, have demonstrated an improved ability to detect hidden arrhythmias compared with Holter monitors (Manta, et. al, 2020). Health data are an important part of maintaining people's privacy. However, in COVID as the above example mentioned, real-time transport of the data to the hospital will harm people's right to privacy, because when they want to hide part of the data being collected by these ECG patches, they will lose the opportunity to do so.

Customers are already using the facial recognition software Alipay to pay at Kentucky Fried Chicken (KFC) restaurants in China and Russia (Liébana-Cabanillas, F, 2022). People are becoming used to the use of biometric technologies in the business scenario. However, it is essential for companies to follow the principle of least authority (PoLA) or the principle of least privilege (PoLP). This principle means that any user, program, or process should have only the bare minimum privileges necessary to perform its function (Digital Guardian, 2023). It is essential to regulatory legislation for information processors. When the privilege of the information collection is at the lowest level, the risk for the information owner will be at the lowest level as well.

### 4.5 The relationship between law and privacy

Professor Guo Bin and his family refused to update their fingerprint recognition to facial recognition for Hangzhou Safari Park, which is a new requirement after they registered for the annual pass (Du & Liu, 2021). This example supports that the wide usage of biometric technologies is indeed affecting people's privacy. Based on the interviews, both participants agree that the law should protect people's privacy. However, it is surprising that both of them believe that with the trend of developing biometric technologies in Chinese society, their right to privacy may need to be given up. The right to privacy is essential to people in the world. They are clarified as the basic right for protecting us to live in this world. To help people establish an understanding of the right to privacy under the legislation system, the author suggests the following method.

First, a clearer definition of the term privacy in all laws. China in 1986 promulgated General Principles of the Civil Law of the People's Republic of China (GCPL). Under the GPCL, privacy is not recognized as an independent right (Ong, 2011). Having a clearer definition that can be applied to most situations is essential and will help people to understand what the regulations are, assist lawyers to clarify their actions, and help judges to make their final decisions.

Moreover, since the lack of one specific law to protect people's right to privacy or human rights. As above literature review mentioned, China now haven't had a law focused on the protection of people's human rights. This may cause Chinese people lack knowledge of how to protect their human rights, which include right to privacy. Moreover, when judges need to make decisions, they don't have the legal basis to make verdict.

On the other hand, a clear calculation method of how much fine should be charged in each case to increase people's awareness will help to raise people's awareness. If someone infringes upon another's privacy or other personality interests, and the aggrieved party, taking tort as the cause to get compensation for spiritual damage, brings a suit to a People's Court, the People's Court shall accept it according to law (Huai, 2005). Currently, legislation about people's right to privacy in China doesn't provide a specific measure of indemnity. Principles as grounds for interpreting laws (Raz, 1971). This causes trouble to people whose privacy is being violated since the lawyer will argue again and again for compensation and use a lot of time, energy, and money.

### 4.6 Suggestions on using biometric technologies

When using biometric technologies, especially in the financial and education fields, ensuring the protection of people's personal data is crucial. Companies should not require or force customers or participants to use their new biometric-related products. Forcing people to agree to the use of biometric technologies' products and treatment violates people's right to privacy. Instead, companies should provide as much information as possible to help people

ISSN 2959-6149

make informed decisions about whether to use biometric-related products.

The expanding use of biometric facial recognition databases and systems must be clearly and demonstrably justified in terms of efficiency and effectiveness for specific security and/or safety purposes, rather than simply appealing to general community security or safety (Smith & Miller, 2021). This approach helps protect people's privacy. Moreover, when new technologies emerge, they often lack the information needed for further development. Therefore, it is important to clearly define the purpose of the technology at this stage (Ceyhan, 2002). When people know the purpose of using certain biometric technologies, they can better monitor the use of these techniques and safeguard their personal information.

To alleviate users' concerns about privacy safety, companies need to enhance supervision. They can use template protection methods, which are permitted to perform identity comparisons using protected representations of biometric templates. These methods can be classified into three categories: cancelable biometrics and cryptographically secure methods (Labati et al., 2012). These methods can improve the security level of a technology by actively comparing different human characteristics. However, there are two opposing views on how to address this issue. Some people believe that it is better not to upload any personal information to technology to protect privacy. On the other hand, some think that producers can collaborate with companies from different fields and government agencies to update information regularly. However, this may lead to more privacy exposure to companies and generally increase the risk of privacy leakage.

## 5. Evaluation

This research successfully analyzes the how biometric technologies affecting people's privacy in contemporary Chinese society. In this dissertation, the author mainly includes three types of biometric technologies, which are facial recognition, iris recognition, and fingerprint recognition.

Based on both primary and secondary research result, the author finds that biometric technologies, for example facial recognition, can bring benefits such as faster digital payment and login process is also dangerous when they are being used for surveillance. Before using facial recognition, it is essential for collecting consent from users. However, relying on consent as the legal basis can be challenging in situations where live facial recognition cameras are used to capture images of significant numbers of people as they pass through public places such as shopping centers or transport interchanges (Harwood, 2024).

Moreover, the occurrence of biometric technologies is affecting Chinese SCS. China has also partnered with the private sector to integrate facial recognition and machine learning technologies with the SCS (Iftimie, et. al, 2020). The use of biometric technologies in the legislation related system also raises new problems and challenges in how to regulate these technologies.

## 6. Conclusion

When Alphonse Bertillon and other French police officers developed the anthropometry system, the development of biometric technologies began. Today, biometric technologies present in almost every field of our life, business, legislation, and so on. The development of biometric technologies in China is unstoppable and the use of it is inevitable.

Living in this background of time, it is essential for us to notice that biometric technologies aren't perfect. Our privacy as a main concern related to the use of biometric technologies is being largely affected. How could people protect our privacy? How do people have our right to privacy? The answer might be people still need to perfect the technologies and guide the development of these technologies.

Regulation is a relatively new term and phenomenon that is being raised up currently in Chinese society. There is a long journey for us to completely take control of the development. The legislation system needs to be revised to fit the current situation. The awareness of the biometric technologies' development needs to be raised. The understanding of the importance of privacy needs to be raised as well. A lot of things are waiting and needing for perfection.

As the legal system and technology develop with time, more people should practice and participate in protecting their own rights of privacy and make informed decisions when giving consent to use different biometric technologies.

In conclusion, biometric technologies are affecting people's privacy by bringing both advantages and disadvantages to people in contemporary Chinese society.

## References

Alenizi, A.S. and Al-Karawi, K.A. (2022) Effective biometric technology used with big data. In Proceedings of Seventh International Congress on Information and Communication Technology: ICICT 2022, London, Volume 3 (pp. 239-250). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-2394-4_22

Alsaadi, I.M. (2015) Physiological biometric authentication

systems, advantages, disadvantages and future development: A review. International Journal of Scientific & Technology Research, 4(12), pp.285-289.

Arista, W.P., et. al (2024) Exploring the Spectrum of Biometric Technologies: A Systematic Literature Review of Conventional and Unconventional Modalities, Procedia Computer Science, volume 245, page 8-18. https://doi.org/10.1016/j.procs.2024.10.224

Biometrics Institute (2020) COVID - 19: Effective and responsible biometrics solutions and concepts in a time of pandemic – building a resilient response. https://www.biometricsinstitute.org/?smd_process_download=1&download_id=6110

Calzada, I. (2022) Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL), Smart Cities, 5(3), 1129-1150. https://doi.org/10.3390/smartcities5030057

Cambridge Dictionary (2025) Law, Cambridge Dictionary. https://dictionary.cambridge.org/dictionary/english-chinese-simplified/law

Carlaw, S. (2020) Impact on biometrics of Covid-19, Biometric Technology Today, 2020(4):8-9. doi: 10.1016/S0969-4765(20)30050-3

Cavoukian, A., et al (2012) 'Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment', Review of Policy Research. https://doi.org/10.1111/j.1541-1338.2011.00537.x

Ceyhan, A. (2002) Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics, Surveillance & society, 5(2). https://doi.org/10.24908/ss.v5i2.3430

Civil Code of the People's Republic of China, c. 4. https://regional.chinadaily.com.cn/pdf/CivilCodeofthePeople'sRepublicofChina.pdf

Dass, S. (2013) Fingerprint-Based Recognition, International Statistical Review. doi:10.1111/insr.12017

Digital Guardian. (2023) What is the Principle of Least Privilege (POLP)? Digital Guardian. https://www.digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance

Donnelly, D. (2024) China Social Credit System Explained – What is it & How Does it Work? Horizons. https://joinhorizons.com/china-social-credit-system-explained/#What_is_Chinas_Social_Credit_System

Du, G., & Liu, H. (2021) China's First Facial Recognition Case, China Justice Observer. https://www.chinajusticeobserver.com/a/china-s-first-facial-recognition-case#google_vignette

Equality and Human Rights Commission (2021) Article 8: Respect for your private and family life, The Human Rights Act. https://www.equalityhumanrights.com/human-rights/human-rights-act/article-8-respect-your-private-and-family-life

Facial Recognition Hardware to Feature on over 800m Mobiles by 2024, Juniper Research. https://www.juniperresearch.com/press/facial-recognition-hardware-to-feature-on-over-800/

Harwood, S. (2024) Big Brother is watching you: Facial recognition in the UK, Stephenson Harwood. https://www.stephensonharwood.com/insights/big-brother-is-watching-you-facial-recognition-in-the-uk

Ho, S. (2015) Maybank launches biometric authentication for mobile banking, The Edge Malaysia. https://theedgemalaysia.com/article/maybank-launches-biometric-authentication-mobile-banking

Huai, L. Y. (2005) Privacy and data privacy issues in contemporary China, Ethics and Information Technology 7:7–15 DOI 10.1007/s10676-005-0456-y

Jain, A. K., & Kumar, A. (2012). Biometric Recognition: An Overview. Second Generation Biometrics: The Ethical, Legal and Social Context, 49–79. doi:10.1007/978-94-007-3892-8_3

Konvitz, M.R. (1966) Privacy and the law: A philosophical prelude, Law and Contemporary Problems, 31(2), pp.272-280. https://doi.org/10.1016/j.patcog.2011.07.019

Labati, R. D., Piuri, V., and Scotti, F. (2012) 'Biometric privacy protection: guidelines and technologies', E - Business and Telecommunications: International Joint Conference, ICETE 2011, Seville, Spain, July 18 - 21, 2011, Revised Selected Papers, pp. 3 – 19. https://doi.org/10.1007/978-3-642-35755-8_1

Liu, F. (2020) Making Cutting-Edge Technology Approachable: A Case Study of Facial-Recognition Payment in China, NN/g. https://www.nngroup.com/articles/face-recognition-pay/

Manta, C., et. al. (2020) An Evaluation of Biometric Monitoring Technologies for Vital Signs in the Era of COVID-19, Clin Transl Sci, 13: 1034-1044. https://doi.org/10.1111/cts.12874

Mascellino, A. (2022) 'Cisco report: 81 percent of all smartphones have biometrics enabled', Biometric Update. https://www.biometricupdate.com/202211/cisco-report-81-percent-of-all-smartphones-have-biometrics-enabled

Maskey, R. (2024) Integrating Biometric Security into Digital Payment Solutions: Opportunities and Challenges, Aitoz Multidisciplinary Review, 3(1), pp.306-312. https://aitozresearch.com/index.php/amr/article/view/88

Metz, R. (2019) If your image is online, it might be training facial-recognition AI, CNN Business. https://edition.cnn.com/2019/04/19/tech/ai-facial-recognition/index.html

Mishra, A., and Dash, S. S. (2023) Unlocking the magic of facial recognition: empowering security and emotions with SVM, Journal of Data Acquisition and Processing, 38(2), p.2402. DOI: 10.5281/zenodo.776955

Newman, L. H. (2022) Chinese Police Exposed 1 Billion People's Data in Unprecedented Leak, Wired. https://www.wired.com/story/chinese-police-exposed-1-billion-peoples-data/

Ogbanufe, O., and Kim, D. J. (2018) Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, Decision Support Systems, 106, 1–14. https://doi.org/10.1016/j.dss.2017.11.003

Oll, Natural Rights. https://oll.libertyfund.org/quotes/epictetus-

ISSN 2959-6149

on-one-s-inner-freedom-that-is-immune-to-external-coercion-c-100-ce

Ong, R. (2011) Recognition of the right to privacy on the Internet in China, International Data Privacy Law, 1(3), 172-179. doi:10.1093/idpl/ipr008

Pascu, L. (2020) Biometric facial recognition hardware present in 90% of smartphones by 2024, Biometric Update. https://www.biometricupdate.com/202001/biometric-facial-recognition-hardware-present-in-90-of-smartphones-by-2024#:~:text=By%202024%2C%20biometric%20facial%20recognition,fingerprint%20sensors%20by%202024%20globally

Perez, J. (2022) Understanding biometric authentication: advantages and disadvantages, Recordia. https://recordia.net/en/understanding-biometric-authentication-advantages-and-disadvantages/#:~:text=Biometric%20authentication%20is%20an%20effective,false%20positives%2C%20and%20high%20costs

Raz, J. (1971) Legal Principles and the Limits of Law, Yale. LJ, 81, p.823. https://heinonline.org/HOL/LandingPage?handle=hein.journals/ylr81&div=37&id=&page=

Sabbagh, D. (2020) South Wales police lose landmark facial recognition case, The Guardian. https://www.theguardian.com/technology/2020/aug/11/south-wales-police-lose-landmark-facial-recognition-case

Slotta, D. (2024) Mobile payment usage rate in China 2016-2023, Statista. https://www.statista.com/statistics/1243879/china-mobile-payment-penetration-rate/#:~:text=Mobile%20payment%20usage%20rate%20in%20China%202016%2D2023&text=As%20of%20December%202023%2C%20the,reached%20also%20a%20high%20level

Slotta, D. (2024) Number of CCTV cameras in leading Chinese cities 2023, Statista. https://www.statista.com/statistics/1456936/china-number-of-surveillance-cameras-by-city/#:~:text=Published%20by,the%20density%20of%20CCTV%20cameras

Smith, M., & Miller, S. (2021) The Ethical Application of Biometric Facial Recognition technology, AI & Soc 37, 167–175 (2022). https://doi.org/10.1007/s00146-021-01199-9

Tangai, M.M., Kaguta, R.J.N. and Yi, Y., (2019) Effect of Ease of Use and Fallibility of Biometric Fingerprint Technology in Criminal Identification in Kenya. https://41.89.227.156:8080/xmlui/handle/123456789/879

Tiwari, S., Chourasia, J.N. and Chourasia, V.S., 2015. A review of advancements in biometric systems. International Journal of Innovative Research in Advanced Engineering, 2(1), pp.187-204. https://d1wqtxts1xzle7.cloudfront.net/36584452/30.JAEC10091-libre.pdf?1423574424=&response-content-disposition=inline%3B+filename%3DA_Review_of_Advancements_in_Biometric_Sy.pdf&Expires=1741266066&Signature=I05HdWwyCS~LE-c17mZ182SYRmsuuag0kphtpJxIJot7wAhJwjfYjnnOLeWAkOQHjVvDY-hSpKT9tSr4Y5FlubK~bRQYyDlC-B5RCS4xmQcSYu2lEQyYfbp-Cu-Yno01KjfrcGUPqlHQ3xO~eG~UzyGyCRJ8PtfUkLmURvqcEojaoJNJ0hGHYOmE0-os4RJQC2Ldrxnseeg2L4DgZVQNcSPXP-zq0SjnImBGVniWDKUnxwkH3hXUXLREdDQrOVnpQGgqcYHInXloA~iU7I7R3fuXSEXpyNLGwUhLwxrAapDgI8jQCVpHlcGsy39AzRjCi3yyJcnZN-s-yhZoB7Zuew__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

UC San Diego UC San Diego Privacy Principles. https://privacy.ucsd.edu/guiding-principles/index.html

Unar, J.A., Seng, W.C., and Abbasi, A. (2014) A review of biometric technology along with trends and prospects, Pattern recognition, 47(8), pp.2673-2688. https://doi.org/10.1016/j.patcog.2014.01.016

United Nations, Universal Declaration of Human Rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=The%20Universal%20Declaration%20of%20Human%20Rights%20(UDHR),document%20in%20the%20history%20of%20human%20rights.&text=Everyone%20is%20entitled%20to%20all%20the%20rights,social%20origin%2C%20property%2C%20birth%20or%20other%20status

Vacca, J.R. (2007) Biometric technologies and verification systems, Elsevier. https://books.google.com.tw/books?hl=en&lr=&id=Pwv_4mnIRFEC&oi=fnd&pg=PP1&dq=what+is+biometric+technology&ots=L6IHSP7H_u&sig=8euwDavDzO77cx2661bCFS1_mVY&redir_esc=y#v=onepage&q=what%20is%20biometric%20technology&f=false

Williams, G.O. (1996) Iris Recognition Technology, IEEE. 10.1109/CCST.1996.551842

Woolf, M. (2025) 29+ Biometrics Statistics for 2025, photoAiD. https://photoaid.com/blog/biometrics-statistics/?srsltid=AfmBOoo_TBWr94WixUBjKd7k0po7dByNKqOfYjEnQ11sPBbgFi6uz070

Xiong, Y., Ritchie, H., & Gan, N. (2022) Nearly one billion people in China had their personal data leaked, and it's been online for more than a year, CNN. https://edition.cnn.com/2022/07/05/china/china-billion-people-data-leak-intl-hnk/index.html

Zhang, C. (2024) Five men passed sentenced for using "AI for face" to manipulate system data for profit, Guangzhou Daily, [online]. https://gzdaily.dayoo.com/h5/html5/2024-07/29/content_872_864561.htm