# IMPROVEMENT OF CHINA'S PERSONAL INFORMATION PROTECTION LAW: THE CASE OF YOUTHS' FINGERPRINT SYSTEM

**[1]Zhaoxun* & [2]Qian Hailu**
Faculty of Culture and Education, Jingdezhen Vocational University of Art, Jing De Zhen, 333000, China
*Corresponding author: caozhaoxun@163.com

**Published online:** 30 November 2023
**To cite this article:** Zhaoxun., Hailu., Q., Improvement Of China's Personal Information Protection Law: The Case Of Youths' Fingerprint System**.** *Asia Pacific Journal of Youth Studies* (APJYS), *2*(2), 115-133. https://doi.org/10.56390/apjys2023.1.1.9
**To link to this article:** https://doi.org/10.56390/apjys2023.1.1.9

## ABSTRACT

Fingerprint identification technology is currently being utilised in variety areas. Although China issued the Personal Information Protection Law in 2021, which addressed several legal and ethical difficulties in this sector, the protection of youths' private information, particularly fingerprint information, remains inadequate. This research uses qualitative research methods to investigate the issue, including case analysis, secondary document review and comparative law method. We studied certain literature and questioned Chinese experts about how they see the public disclosure of fingerprint information of today's youths and how they perceive the legal laws of fingerprint identification technology for youths, after analysing examples from the US, the EU, and France. Concerning the findings, it is important to note that incidents of fingerprint systems for adolescents have been described as prevalent and dangerous. Futher more, the current protection of fingerprint information involving youth still needs to be improved in China's legislation. In China's current legislative system, there is a lack of protection of fingerprint information of youth in the Civil Code, the Network Security Law, and the Personal Information Protection Law. Finally, to solve this problem,

diversified legal governance approaches can be tried. For example, refining the relevant provisions of the Personal Information Protection Law, strengthening cyber justice, and enhancing citizens' legal education. Multi-level coordination to control the leakage of fingerprint data and protect the privacy of citizens, especially youth.

***Keywords:*** Youth, Fingerprint Identification System, Information Protection Law, China, Privacy Rights

## INTRODUCTION

### *Research Background*

Zhang Yaping(2020) notice that fingerprint identification technology is a form of biometric authentication technology, which is designed to accurately identify individuals by analysing the unique patterns present in their fingerprints. Zhou Weilong (2019) discovered that fingerprint identification technology matches a person to his fingerprints, and that by comparing his fingerprints to pre-saved fingerprints, his genuine identity can be verified. The patterns, breakpoints, and intersections of each person's skin pattern, including fingerprints, are unique, and we rely on this uniqueness and stability to produce fingerprint identification technology. Each individual's skin pattern, including fingerprints, differs in pattern, breakpoints, and intersections and is unique and constant throughout life.

The origins of the contemporary examination of fingerprints may be traced back to the 19th century, when Francis Gahon, in his publication titled "Fingerprint," identified the distinctive and consistent qualities of fingerprints. Gahon subsequently suggested a systematic classification system for fingerprints based on these observations. This is widely regarded as the inception of contemporary fingerprint science. According to He Amei, Cai Xianling(2023), improvements in technical methods and identification theories have since pushed the evolution of fingerprint identification technology.

In 2012, the Chinese government enacted the Decision on Strengthening the Protection of Network Information, which explicitly affirms the state's responsibility to safeguard electronic data that can identify individuals and pertains to their personal privacy. Consequently, the technology of fingerprint identification started to gain public attention.

***Problem Statement***

Is youth fingerprint protection important? Fingerprint identification technology has been widely employed in the development of "Digital China" in a variety of industries. However, many privacy, legal, and ethical issues have yet to be addressed in the design and implementation of the youth fingerprinting system, resulting in a variety of youth information leakage difficulties. The following are the primary reasons for the leakage of fingerprint information in China. For starters, counterfeit or cloned fingerprint samples may readily tamper with fingerprints throughout the gathering procedure. Second, there are no uniform fingerprint data protection rules in place. Furthermore, there is a dearth of explicit advice on youth legal literacy and associated instruction in school. According to Stitilis D. (2023), in a research aimed at the European Union, it looks risky to build a system of fingerprinted evidence protection utilising biometric data as defined by the General Data Protection Regulation (GDPR) as a special legal framework. Furthermore, in the United States, schools provide universal standards for personal information protection as well as differentiated data protection. Providing uniform personal information standards, diversified approaches for personal information protection, and improving data personal information protection legislation, among other things, to better safeguard youths' personal information security. The disclosure of youths' fingerprint information has posed significant concerns to the security of personal information, the protection of life and property, and the security of social government. The safeguarding of youths' fingerprint information has reached a point where the government must step in. How to regulate the scope and standard of use of youth fingerprint information through legislation, and how to build a legal system of youth fingerprint information to protect youth

information while safeguarding technological development, are critical issues that must be addressed in theoretical research and practical application.

***Research Question***

As previously indicated, it is evident that safeguarding the personal information of youth is a matter of great significance. The safeguarding of fingerprint information, a sort of biometric data pertaining to persons, is currently of paramount importance. The primary objective of this study is to investigate the aforementioned concerns.

1. What factors contributed to success of keeping up the security of fingerprint data among youths in China?
2. What are the mechanisms that can safeguard the fingerprint data from get infringed by manipulators?

***Research Objective***

This study will collate the views of the literature related to the protection of fingerprint information of adolescents, as well as the observation of typical cases, in order to systematically elaborate the current limitations in the protection of fingerprint information of adolescents. On the basis of the previous studies, suggestions for solutions will be made to fill the gaps in the relevant research.

***Research Framework***

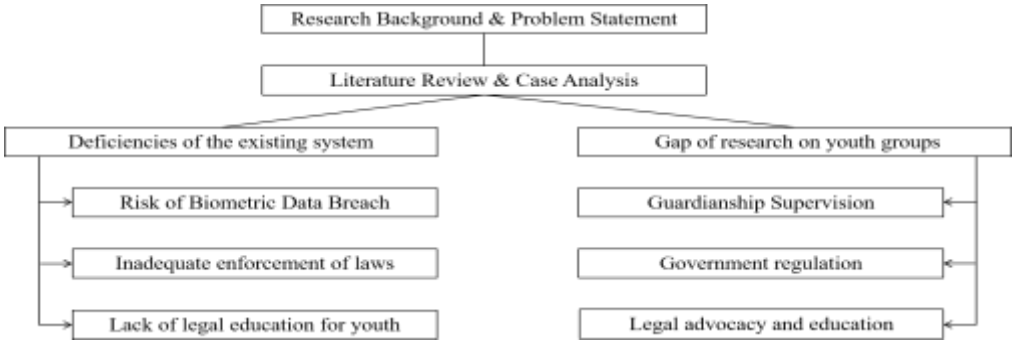


**Figure 1.**
*Research Framework*

## LITERATURE REVIEW

Presently, a considerable number of researchers are engaged in the investigation of fingerprint recognition technology. In "Development and Application Status of Fingerprint Identification Technology", He A-Mei (2023) discuss the development history, status quo, and specific application scenarios of fingerprint identification technology by sorting out the relevant policies of the state. The authors of this paper examine the existing shortcomings of fingerprint identification in terms of technology, application, and security. They subsequently provide potential solutions to address these flaws and offer a roadmap for the advancement of sectors associated to fingerprint identification technology. Xu Zibo (2020) explores the advantages and limitations of the current ID card fingerprint collection as well as its application from the perspective of criminal justice in his exploration of the application of second-generation ID card fingerprint information in the detection of murder cases. Lv, Daozhong (2018) mentions the current risks in fingerprint identification in China in his study "On the Risks of Fingerprint Identification under the Condition of Big Data". Zhang Jianwen and Pan Linqing (2018) talk about strategies to achieve a rational balance between fingerprint information protection and civil identity proof in the article "The scope, dilemmas and solutions to the legal protection of fingerprint information in applying for resident identity cards". And Pan Linqing (2018) points out the problems that exist in the registration of fingerprint information by citizens in his paper "On the Legal Protection of Fingerprint Information - Taking the Registration of Fingerprints in China's Resident Identity Card Receipt as an Example".Štitilis, D., Laurinaitis, M. and Verenius, E. (2023) in Securing Critical Infrastructures with Biometrics: a Context for the Protection of Personal Data, present recommendations for the introduction of a specific legal framework for the processing of biometric data in the context of the protection of critical infrastructures. It is evident that a significant portion of scholarly study pertaining to fingerprint information and fingerprint recognition technology primarily focuses on the examination and investigation of technological aspects. In the context of the fingerprint information case

study, the investigation pertaining to the youth as a distinct demographic subgroup appears to be somewhat limited in scope. Using the CNKI Chinese literature database as a case study, a comprehensive search was conducted for research literature pertaining to "fingerprint identification technology" in China throughout the period of five years (2019-2023). This search yielded a total of 441 relevant scholarly articles. Through the process of categorization, it becomes evident that the primary focus of the material encompassed within the specified search parameters pertains to the field of fingerprint identification technology.(Diagram 1)When the CNKI Chinese database was searched for "minors' fingerprints", "adolescents' fingerprints" and "children's fingerprints", no search records were found for this particular subject. In other words, there is no record of this particular subject in the current research in China. In other words, "minors" are not treated as a special subject in China's current research. However, this improvement of china's personal information protection law:the case of youths' fingerprint system
argues that minors possess natural characteristics that distinguish them from adults. As one of the special subjects of legal discussion, the protection of fingerprint data of minors is an indispensable topic.

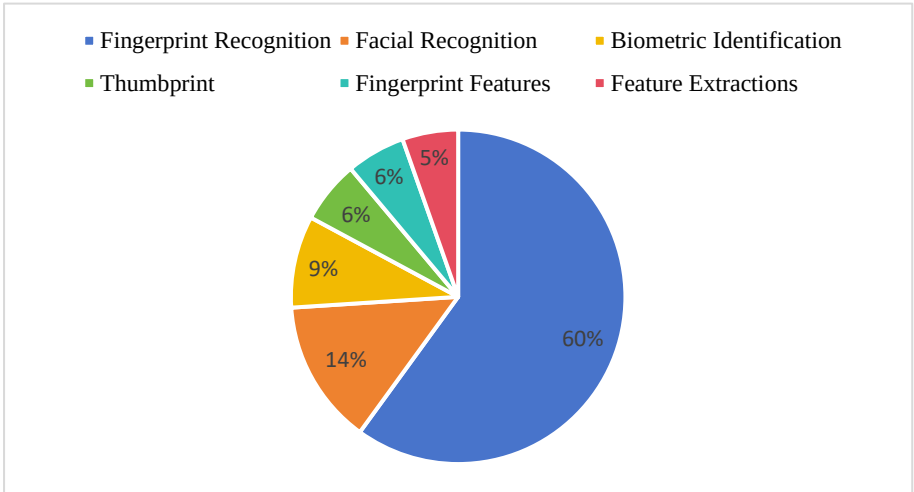


**Figure 2.**
Results of the Subject of "Fingerprint Recognition Technology"

## METHODOLOGY

This study adopts a qualitative research methodology to examine the protection of fingerprint information of youths. The research will employ comparative case research and secondary document analysis methodologies.

### *Comparative Case Research*

This study seeks to investigate the tactics employed for safeguarding the fingerprint data of youths via the lens of empirical legal analyses. It will accomplish this by evaluating representative cases that involve the unauthorised disclosure of fingerprint information belonging to youths, both within and outside the relevant jurisdiction. The empirical legal analysis technique offers a distinct benefit by facilitating an exploration of pertinent cases, so enabling a more intuitive assessment of the phenomenon surrounding a specific legal matter. Hence, this research aims to analyse the factors contributing to instances of youths' fingerprint leaking by investigating both domestic and foreign cases.

### *Secondary Document Analysis*

This study seeks to examine the existing scholarly research on safeguarding the fingerprint data of children and establish a more uniform framework for protecting such information through the application of normative legal research methodologies.

## DISCUSSION AND FINDING

### *Comparison: From the USA* and Fransh

During the period of 2019-2021, the United States House and Senate have introduced measures that pertain to the regulation of fingerprint identification technology. Furthermore, pertinent legislation has been implemented at both the state and local government levels inside the United States. The legal regulation of fingerprint identification technology in the United States is primarily focused on striking a delicate equilibrium between safeguarding the protection of

individuals' personal information and fostering the advancement of biometric technology. These laws exhibit greater comprehensiveness and impose more severe penalties. Furthermore, they encompass various perspectives by implementing restrictions and prohibitions on the utilisation of the technology. Primarily, they mandate that enterprises employing fingerprint identification technology must obtain explicit consent from users and restrict their authority to collect and store fingerprint information. In addition, it is important to note that there exist limitations on the utilisation of fingerprint identification technology by governmental entities. Specifically, law enforcement organisations are prohibited from employing such technology for surveillance purposes unless proper authorization has been granted. In the current era characterised by swift technology advancements, there exists a compelling impetus for China's legislative endeavours. It becomes imperative to expedite the growth of the digital economy while concurrently formulating judicious legal frameworks to safeguard the lawful rights and interests of its populace. Hence, it is incumbent upon the legislative body to strive for equilibrium between the competing interests at hand and to craft legislation with a sense of anticipation.

And the concept of informed consent under the United States Children's Online Privacy Protection Act (Coppa) depends largely on the use of "verifiable parental consent" as a means of protecting children's information-related rights. The term "verifiable parental consent" refers to the requirement that entities responsible for the collection, use, disclosure and further exploitation of a minor's personal information inform and obtain the consent of the child's parent or legal guardian.

The French Data Protection Authority has also indicated that objectives must be set in accordance with the necessity of biometric systems: firstly, biometric systems directly related to necessary and non-refusable security measures (personal identification, etc.); secondly, biometric systems as related services (commercial products, etc.) - where users must be duly informed and required to submission

of obvious protocols for the use of their biometric data and the provision of alternative options; and thirdly, biometrics used to conduct research and experiments. The choice of technology and the adequacy of the biometric data are required in each case to achieve the stated objectives.

***China's Policy on Youth Fingerprint Information Protection***

Currently, China lacks a distinct legal framework specifically addressing the collection and management of fingerprint data pertaining to individuals under the age of majority. The level of protection afforded to minors' personal information in China is comparatively inadequate. The Cybersecurity Law was enacted by the Standing Committee of the National People's Congress (NPC) in 2016. It has extensive regulations pertaining to the safeguarding of personal information, as outlined in the chapters addressing "network information security" and "network operation security". The year 2020 is widely recognised as the inaugural year of China's legislation pertaining to the protection of personal information. Since then, there has been a consistent effort to enhance and advance the laws governing personal information protection. In the year 2020, commonly referred to as the inaugural year of China's personal information protection laws, efforts will persist in enhancing and advancing the personal information protection law. The Personal Information Protection Law of the People's Republic of China enacted in 2021 encompasses the safeguarding of personal information pertaining to children. However, it lacks comprehensive legislative provisions specifically addressing the protection of fingerprint information.Nor does it reinforce the principle of guardian consent and establish the principle of guardian recovery.

***Separate Legislation and establishment of the "notice-consent" principle***

Propose distinct legislation aimed at enacting a legal framework for safeguarding the fingerprint data of individuals under the age of majority, while concurrently establishing the responsibility and liability of legal guardians in this regard.

China lacks specific provisions regarding the safeguarding of minors' personal information in significant legal frameworks such as the Civil Law and the Criminal Law. The existing regulations merely offer general provisions on personal information protection, primarily relying on the consent of guardians. Hence, instances of fingerprint information leakage are addressed by considering the provisions outlined in pertinent legislation concerning the protection of personal information, including the Personal Information Protection Law, the Protection Provisions, the Civil Code, and others. However, these regulations are somewhat scattered and lack specificity, allowing perpetrators to exploit legal loopholes through the utilisation of advanced technology. Consequently, the privacy rights of minors are persistently violated, leading to disruptions in their daily lives. We can then learn from the United Kingdom and the United States, which have enacted separate legislation to promulgate a corresponding legal framework.

When formulating legislation concerning the safeguarding of fingerprint data belonging to youth, it is imperative to adhere to the idea of prioritising the welfare and best interests of individuals under the age of majority. The establishment of the 'notification-consent' principle is crucial in creating the safeguarding of fingerprint information belonging to children. This principle serves as a significant mechanism for ensuring that individuals are adequately informed and empowered to make decisions regarding the processing of their minors' information. This Law places emphasis on the adherence to certain principles when processing fingerprint information of minors. These principles include legality, legitimacy, necessity, and good faith. The processing must have a clear and reasonable purpose that is directly relevant to the processing itself. Additionally, the method employed should minimise any negative impact on the rights and interests of the individual. The processing should be limited to the smallest extent necessary to achieve its intended purpose. Furthermore, the rules governing the processing should be disclosed, the quality of the information should be ensured,

and appropriate security and protection measures should be implemented. These principles are to be consistently applied throughout the entire process of handling minors' information. These rules must to be implemented consistently throughout the entirety of the process of managing minors' information, encompassing all facets of the procedure. These rules ought to be implemented consistently throughout the entirety of the procedure for managing information pertaining to minors, encompassing all phases of the process.

***Structuring the guardianship recovery system***

However, upon the implementation of the pertinent legislation, it is imperative to enhance the principle of guardian consent and establish the idea of guardian recourse. This principle is grounded in two primary factors. Firstly, individuals under the age of 14, commonly referred to as minors, may exhibit either an inability or limited capacity to engage in civil behaviour. Consequently, their ability to make rational judgements regarding the potential consequences associated with the disclosure of personal information is compromised. As a result, the involvement of their legal guardians is necessary to safeguard these minors. Furthermore, this aligns with the stipulations outlined in the Civil Code and the Law on the Protection of Minors. According to Article 1,035 of the Civil Code, it is explicitly stated that the processing of a minor's information necessitates the consent of their guardian. Additionally, Article 72 of the Law on the Protection of Minors specifies that when handling personal information of a minor below the age of fourteen, the consent of the minor's parents or legal guardian must be obtained, unless there are specific provisions in the law or administrative regulations that state otherwise. Due to the deceptive tactics employed by certain minors, who exploit guardians' lack of awareness to gain access to electronic products or software, there is a risk of inadvertently exposing their personal information. In cases where guardians fail to adequately supervise and consequently allow the disclosure of minors' relevant information, they should be held accountable for their responsibilities as guardians.

Currently, there is a lack of explicit guidelines in China

regarding the particular methods for getting the approval of a guardian. In terms of a comparative analysis, it can be observed that the principle of guardian consent in the United States is functioning pretty effectively. China has the opportunity to examine and derive insights from the implementation of the United States' Children's Online Privacy Protection Act (COPPA). The idea of informed consent under the U.S. Children's Online Privacy Protection Act (COPPA) primarily hinges upon the utilisation of "verifiable parental consent" as a means to safeguard the rights pertaining to children's information. The term "verifiable parental consent" refers to the requirement for the entity responsible for collecting, using, disclosing, and further utilising personal information of minors to inform and obtain consent from the parents or legal guardians of the child. This obligation takes into consideration the advancements in technology.

Minors typically rely on their legal guardians for information processing. Therefore, it is imperative to build a system that allows for recourse to guardians, enhance family guardianship, and ensure that legal guardians fulfil their basic responsibilities. In order to enhance the safeguarding of minors' personal information, it is imperative to enhance the oversight mechanism for guardians, establish a dedicated organisation to evaluate and monitor guardians' aptitude for guardianship, and establish alternative guardianship entities.

The safeguarding of minors should not be solely seen as a private concern within families. By implementing a nationwide guardianship system, the care and protection of youngsters should be recognised as a societal issue, allowing for the involvement of all members of the community. The presence of a dedicated governing body responsible for overseeing and protecting guardianship has considerable importance in guaranteeing the establishment of proper responsibilities and the effective implementation of supervisory obligations and safeguards. Parents, in their capacity as legal custodians of their underage offspring, bear a legal duty to ensure the physical well-being of the minor. In the event that a parent neglects this role and inflicts bodily injury upon the young, they should be held

accountable under the law, either through legal responsibility or criminal liability. When crafting legal provisions, it is imperative to consider and refine all relevant conditions.

***Strengthening oversight and improving the oversight system***

Currently, there is a deficiency in the safeguarding of personal data in China, despite the existence of a pertinent provision in Article 60 of the Personal Information Protection Law. This provision designates the State Net Information Department as the responsible entity for coordinating efforts pertaining to the protection of personal information, as well as overseeing and managing related activities. The protection of personal information and monitoring and administration within their respective areas of responsibility are the duties assigned to the appropriate departments of the State Council, as stipulated by this Law and other applicable laws and administrative rules. In actual implementation, the supervisory strategy of "coordination by the national Internet information department and separate enforcement by the relevant departments of the State Council" has proven to be ineffective in safeguarding minors' personal information. This approach has failed to adequately prevent the arbitrary collection and subsequent leakage of minors' personal data, leading to occasional instances of infringement upon their privacy.

In summary, the oversight conducted by the Government has been insufficient. It can be considered to establish a monitoring and reporting mechanism as the primary step. This mechanism would enable citizens to collectively oversee the functioning of the fingerprint system for minors. Subsequently, if a citizen reports any perceived unreasonableness in the system's operation, it is recommended that investigations be intensified. Furthermore, efforts should be made to prompt the correction and enhancement of the system based on the findings of these investigations. And it is imperative to enhance media oversight in the current era of information-based internet. Media supervision can effectively fulfil its supervisory duty and act as a catalyst for social organisations and other entities, thereby facilitating the implementation of the fingerprint

system for minors and promoting social oversight.

It is imperative for the government to enhance its oversight mechanisms, establish a comprehensive system for safeguarding the information of minors, establish a robust framework for protecting personal data, establish dedicated agencies, foster greater collaboration among relevant departments, and intensify supervision across all domains. These measures are crucial in order to minimise instances of infringement upon the rights of minors.

Furthermore, it is imperative to limit the economic pursuits of firms by emphasising the need for enterprises to proactively undertake social responsibilities, enhance their internal management practises, bolster their resilience against hazards, prevent unauthorised access, and safeguard the personal information of users. However, it is imperative for industry creators to ensure comprehensive disclosure during sessions, encompassing crucial aspects pertaining to the rights and interests of all involved parties. This includes divulging information regarding the content, extent, utilisation, intended methodology, and collection of personal data, as well as addressing the rights of minors and avenues for seeking redress. Additionally, it is essential to emphasise the significance of safeguarding the personal information of minors and other related matters. The protection of minors and their guardians' rights to access information and seek legal recourse is comprehensively ensured in order to prevent any infringement upon their rights and interests arising from imbalances in information availability.

***Strengthening education and guidance for young people***

Minors, who are currently undergoing growth and development, often lack a strong awareness of personal information protection. It is imperative for the state, society, schools, and families to collectively address the issue of safeguarding the personal information of minors through educational initiatives. By enhancing the self-protection awareness and capabilities of minors, these efforts aim to assist them in protecting their legitimate rights and interests.

Furthermore, it is imperative for educational institutions to establish an effective framework to safeguard the personal information of underage students. This entails developing innovative mechanisms to protect students' personal information within school premises, fostering collaboration between schools and families, advocating for privacy awareness, and implementing other pertinent recommendations. These measures aim to empower minors with the knowledge and skills necessary to comprehend and safeguard their personal information appropriately.

Enhance the safeguarding of students' entitlement to access information pertaining to their personal data, thereby ensuring their awareness of the possibility for individuals to inquire with relevant institutions regarding the collection and utilisation of their personal information. Additionally, students should be empowered to request the provision of pertinent supporting documentation from said institutions. Individuals possess the entitlement to decline the gathering and utilisation of their personal information by the respective institutions. Individuals have the opportunity to submit requests to the organisation for the deletion or correction of their personal information. It is the responsibility of the organisation to address these requests within the legally prescribed timeframe. This process serves to strengthen the protection of minors and ensure the security of their personal information.

## CONCLUSION

The use of documentary and comparative analysis in research is not a unique strategy, although it has been underutilised in previous studies. Therefore, it is particularly important to use this method in the process of improving the information protection system for adolescents in China. However, since there has been no relevant research on fingerprint information protection for adolescents in China, the conclusions drawn from comparative analyses are rather limited. Nevertheless, we must acknowledge that the rapid advancement of this technology has led to an increasingly pervasive encroachment on our

right to privacy. This erosion has had a clear impact on our daily lives. It is therefore crucial to explore ways to enhance the protection of personal information in any country. In addition, priority must be given to protecting the personal information of adolescents, not only to safeguard their individual rights, but also to be consistent with the relevant legal framework. Both the State and society should pay more attention to this issue and accelerate the implementation of effective measures to promote social harmony. In the studies of relevant scholars, while focusing on the protection of citizens' privacy rights, the special status of teenage citizens is often neglected. Teenage citizens are the most active group of Internet users, who lack legal knowledge and are more likely to disclose their personal information. In addition, this study proposes diversified legal governance ideas. Therefore, this paper puts forward the following suggestions for China in the protection of fingerprint information of adolescents: 1) separate legislation and establishment of the guardian's recourse system; 2) strengthening supervision and improving the supervision system; 3) playing the role of enterprises and society; 4) strengthening the education and guidance of adolescents and so on, which will help to solve the current problem of adolescents' fingerprint data leakage. This study also has shortcomings, namely the lack of social research on the youth population. Therefore, in the next action session, further research can be conducted through questionnaires on teenagers' attitudes towards personal information leakage.

## ACKNOWLEDGEMENT

I express my gratitude to Jingdezhen Vocational University of Art for their support during the completion of this work. I would want to express my gratitude to my mentor, Mr. Cao, for his invaluable instruction. Appreciate his acknowledgement of the importance of the subject matter and their valuable recommendations for the article.

## REFERENCES

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.

Cheng Yan. (2023). Research on the Legal Issues of Network Personal Information Protection in the Information Age. *Time Figures*. *1*(7), 0101-0115.

He A-Mei, Cai Xianling & Chen Minxin. (2023). The development and application status of fingerprint identification technology. *Research on Industrial Innovation*, *3*(6), 102-118.

Huddleston, J. (2023). Would New Legislation Actually Make youths Safer Online? Analyzing the Consequences of Recent Youth Online Safety Proposals. *Cato Institute Briefing Paper*.

Jamison, S. G. (2019). Creating a National Data Privacy Law for the United States. *Cybaris Intell. Prop. L. Rev.*, *10*(1), 1-25.

Liao Jiaqi. (2021). Is based on the framework of the Regulations on the Protection of Children's Personal Information Network. *Library construction*, *000*(002), 98-107.

Liu Quan. (2021). On the legality, legitimacy and necessary principles of personal information processing. *Jurists. 5*(5), 1-28.

Liu Yhao, & Nan Lijun. (2022). Analysis on the necessity and applicability of personal information protection legislation in China. *Journal of Shanxi Datong University: Social Science Edition*, *36(*6), 31-45.

O'Neil, M. M. (2023). The Illinois Biometric Privacy Act: History, Developments, And Adapting Protection for the Future. *Student Journal of Information Privacy Law*, *1*(1), 1-49.

Shen Chuxuan. (2023). Study on the optimization of administrative public interest litigation. *Western Academic Journal*. *3*(4), 104-108.

Wang Dezheng. (2021). Criminal law protection for biometric information: realistic situation and perfect path Take Sichuan "face recognition case" as the entry point. *Journal of Chongqing University: Social Science Edition*, *27*(2), 133-143.

Wang Ya. (2022). The realistic dilemma and path optimization of minors' personal information protection. *Time Law*. *2*(6), 79-94.

Wu Yi. (2022). On the protection and regulation level of personal Information rights and Interests- -Based on the analysis of the relevant functions of the Personal Information Protection Law of the People's Republic of China. *Journal of Guizhou Party School. 2* (6), 120-128.

Xu Sirui, & Wang Yue. (2023). Improvement of the guardian consent system in the protection of minor personal information Based on the analysis of the guardian consent mechanism of 36 apps in China. *Journal of Luoyang Normal University*, *42*(2), 92-100.

Xu Zhibo, Ouyang Zhen, & Ye Xinrong. (2020). Application of second-generation ID card fingerprint information in homicide detection. *Criminal technology*, *45*(6), 3-12.

Yang Yifan. (2023). On the fiduciary obligation of network platform to protect personal information. *The reference of entertainment law. 1* (7), 16-25.

Zhang Junwei. (2023). On the administrative public interest litigation in the field of personal information protection. *Chutian Rule of Law. 2* (13), 0243-0245.

Štitilis, D., Laurinaitis, M. and Verenius, E. (2023). Securing critical infrastructures with biometrics: the context of personal data protection. Issues in Entrepreneurship and Sustainability, *1*(10),133-150.

Štitilis, D., & Laurinaitis, M. (2017). Biometric processing of personal data: issues of harmonised practices under EU personal data protection law. Computer Law & Security Review, *33*(5), 618-628.