Acta Bioethica 2023; 29(2): 249-258. http://dx.doi.org/10.4067/S1726-569X2023000200249

CHALLENGES AND PRINCIPLED RESPONSES TO PRIVACY PROTECTION FROM BIOMETRIC TECHNOLOGY IN CHINA

Yi Zhang[1], Bohua Liao[2], Ruipeng Lei[3]

Abstract: Biometric technology has transformed human biological characteristics into a new form of privacy, and the misuse of this technology poses challenges to protecting this new privacy. This article initially defines biometric technology and biometric characteristics, further demonstrating why biometric characteristics belong to personal privacy and how biometric technology poses challenges to its protection. Through analysis, this article argues that the essence of these challenges is the conflicts between the ethical principle of privacy protection and the ethical principle of maximizing social benefits. In order to address these challenges, it is necessary first to weigh the fundamental ethical principles. The two basic principles of privacy protection and maximizing social benefits are not mutual antagonism but hierarchy, and this hierarchy should be based on the principle of practical feasibility. That is, applying biometric technology should first meet the principle of practical feasibility and, on this premise, realize the principle of maximizing social benefits based on not infringing on the principle of privacy protection.

Keywords: biometrics, biometric technology, biometric characteristics, privacy protection, the hierarchy of ethical principles

Retos y respuestas de principio a la protección de la intimidad por la tecnología biométrica en China

Resumen: La tecnología biométrica ha transformado las características biológicas humanas en una nueva forma de privacidad, y el uso indebido de esta tecnología plantea desafíos a su protección. En este artículo se define inicialmente la tecnología biométrica y las características biométricas; se demuestra además por qué las características biométricas pertenecen a la privacidad personal y cómo la tecnología biométrica plantea retos para su protección. Este artículo argumenta que la esencia de estos retos es el conflicto entre el principio ético de protección de la privacidad y el de maximización de los beneficios sociales. Para abordar estos retos es necesario sopesar primero los principios éticos fundamentales. Los dos principios básicos de protección de la privacidad y maximización de los beneficios sociales no son antagónicos, sino jerárquicos, y esta jerarquía debe basarse en el principio de viabilidad práctica. Es decir, la aplicación de la tecnología biométrica debe cumplir primero el principio de viabilidad práctica y, a partir de esta premisa, realizar el principio de maximización de los beneficios sociales sobre la base de no infringir el principio de protección de la intimidad.

Palabras clave: biometría, tecnología biométrica, características biométricas, protección de la intimidad, jerarquía de principios éticos

Desafios e respostas baseadas em princípios à proteção da privacidade da tecnologia biométrica na China

Resumo: A tecnologia biométrica transformou as características biológicas humanas em uma nova forma de privacidade, e o mal uso dessa tecnologia apresenta desafios para proteger essa nova privacidade. Esse artigo inicialmente define tecnologia biométrica e características biométricas, demonstrando posteriormente por que características biométricas pertencem à privacidade pessoal e como tecnologia biométrica coloca desafios à sua proteção. Através de análise, esse artigo discute que a essência desses desafios é o conflito entre o princípio ético da proteção da privacidade e o princípio ético de maximizar benefícios sociais. De forma a visar esses desafios é necessário primeiro ponderar os princípios éticos fundamentais. Os dois princípios básicos de proteção da privacidade e de maximizar benefícios sociais não são mutuamente antagônicos mas hierárquicos, e essa hierarquia deve ser baseada no princípio da viabilidade prática. Isso é, aplicar tecnologia biométrica deve primeiro atender ao princípio da viabilidade prática e, nessa premissa, compreender o princípio de maximizar benefícios sociais com base em não infringir o princípio de proteção da privacidade.

Palavras chave: biometria, tecnologia biométrica, características biométricas, proteção da privacidade, a hierarquia dos princípios éticos

[1] School of Philosophy, Centre for Bioethics, Huazhong University of Science and Technology, Wuhan, China. The Institute of State Governance, Huazhong University of Science and Technology, China, Wuhan, ORCID: 0009-0008-9636-0073.

[2] School of Philosophy, Centre for Bioethics, Huazhong University of Science and Technology, Wuhan, China, ORCID: 0009-0004-0796-0562.

[3] School of Marxism/Center for Ethics and Governance of Science and Technology, University of Electronic Science and Technology of China, Chengdu 611731, China, hustbioethics@foxmail.com, ORCID: 0009-0003-2553-296X

1. Introduction

In recent years, with the rapid development of underlying technologies such as big data and artificial intelligence, biometric technology in China has become increasingly widespread. From its initial use in specific public safety and criminal investigation fields, it has expanded to various public spaces such as high-speed railways, airports, customs, banks, companies, communities, and various large and small shops. At the same time, the leakage, theft and abuse of personal biometric data have become increasingly severe. In 2019, a face-swapping application called ZAO became popular in China. However, privacy infringement and individual portrait rights were gradually exposed. Because of that, the Ministry of Industry and Information Technology of the People's Republic of China (MIITPRC) inquired about the software operator*(1)*.In October 2019, Hangzhou Wildlife Park adopted facial recognition for admission without justifiable reason. Guo Bing, an associate professor at Zhejiang Sci-Tech University, sued the park after unsuccessful coordination due to concerns about privacy and personal and property rights infringement and eventually won - known as "the first case of Chinese facial recognition"*(2)*. In 2021, China's state media exposed that many well-known stores, including Kohler, BMW and Max Mara, installed facial recognition cameras to secretly collect many personal biometric data from customers*(3)*. Even more outrageous is that some cities have also installed facial recognition systems at public toilets for distributing toilet paper*(4)*. The ubiquitous cameras have caused great panic among people, especially when personal biometric data is obtained, used and traded without their knowledge. At the same time, biometric technology's security and reliability are also highly problematic. According to Tsinghua University's RealAI team report, 19 unfamiliar smartphones can be unlocked in 15 minutes using face recognition vulnerabilities*(5)*.

Biometric technologies such as facial recognition are growing wildly in China, causing many social and ethical problems. For a time, whether biometric technology should be developed and how it should be developed became the most urgent question to be answered. Among all the "justification" arguments for developing biometric technology, privacy protection is an essential ethical argument that cannot be bypassed. The challenges of biometric technology to privacy protection are also the most concerning issue among the ethical problems raised by this technology.

2. The definition of biometric technology and biometric characteristics

Biometric technology is a type of technology that automatically identifies or authenticates an individual's identity based on their unique physiological or behavioral characteristics*(6)*, which are biometric characteristics*(7)*. Among them, the recognition based on an individual's unique physiological characteristics is called classical biometric recognition, which mainly includes fingerprint, facial, iris, vein, DNA, etc.*(8)*.

Currently, the main function of biometric technology is the authentication of individual identity, which is generally accomplished by both authentication and identification. Authentication is a one-to-one comparison by comparing the characteristics provided by a person with the characteristics of the identity he declares*(9)*. This type of authentication allows local storage of biometric characteristics under personal control*(10)*, so users' privacy is relatively secure. Identification is a one-to-many comparison by collecting a person's biometric characteristics and comparing them with the identity characteristics in the database to determine the identity of the person to be identified*(9)*. The database is organized and controlled by one or more controllers with the help of one or more processors. Ultimately, biometric characteristics are no longer under the physical control of users, and they can no longer control how to use them on their own*(10)*. Biometric characteristics as a means of authentication or identification are very reliable because they allow a person to establish a strong relationship between an individual and their identity by verifying unique physical or biological characteristics for independent individuals*(11)*.

The reliability of biometric technology can also be reflected by comparing it with traditional identity recognition. Traditional identity recognition can be roughly divided into two categories: one is through "something you have"*(12)*, that is, phy-

sical objects to identify identity, such as ID cards, passports, keys, smart cards, etc.*(13)*; the other is through "something you know"*(12)*, that is, memorized password or PIN (personal identification number) to identify identities, such as passwords and codes*(13)*. These traditional identity recognitions have security and reliability issues, such as being easily lost, forgotten, copied, and cracked. Nevertheless, biometric technology is based on "something you are"*(12)*, that is, biometric characteristics. It has advantages such as uniqueness, lifelong immutability, portability, difficulty in losing and avoiding misusing, and anti-counterfeiting*(9)* to make up for the shortcomings of traditional identity recognition and make identity recognition more secure and reduce the risk of fraud. Therefore, it has begun to be widely used today. Currently, biometric technology is widely used in public and private sectors, including national security, criminal investigation and detection, account security authentication, financial transactions, and other aspects. Its application purpose is mainly based on social security and convenience.

At the same time, however, many ethical issues are associated with using biometric technology, such as privacy protection, autonomy issues, and social exclusion*(12,14)*. Among these issues, privacy protection is the central and most important concern, which is the focus of this paper.

3. The challenges of biometric technology for privacy protection

3.1. Biometric technology turns human biometric characteristics into a new privacy

Privacy, a fundamental human right, is often directly linked to freedom and autonomy and is a concrete manifestation of respect for human dignity. In biometric technology, privacy can roughly recognize in three different forms: physical privacy, decisional privacy, and information privacy*(15)*. Physical privacy refers to an individual's freedom to refuse contact with others or disturbing by others*(16)*; decisional privacy is the freedom of an individual to make choices that affect personal affairs independently*(17)*; informational privacy is the freedom of an individual to control or have some influence over specific information about oneself*(18)*.

Biometric technology uses an individual's biometric characteristics, which originally existed only as personal biological characteristics. However, due to the emergence and application of biometric technology, these characteristics, which originally existed only as individual characteristics, have become obtainable and have been transformed into personal information. Personal information refers to any information related to a natural person whose identity has been or can be identified, including personal name, address, date of birth, ID number, medical records, personnel records, photographs, and other information that can identify a specific individual when used alone or in conjunction with other information*(19)*. Among all personal information, that which an individual does not wish to disclose to society or be known by others is considered private information. The information derived from an individual's unique physiological or behavioral characteristics and recognized by biometric technology is precisely the part of identifiable personal information that the subject does not want others to obtain. Therefore, we can say that personal biological or biometric characteristics have become the personal privacy of citizens in the current society due to biometric technology.

3.2. Biometric technology poses various challenges to privacy protection

For one thing, by analyzing the technical principles of biometric technology, the use poses a significant potential risk to privacy. This risk is not only due to the possibility that information leakage may be caused by the current imperfection of biometric technology, which can result in loss and harm to the information subject. It is also due to the special properties of biometric characteristics that make such damage and harm, if it occurs, more severe than a general privacy breach. Compared with privacy in the traditional sense, personal biometric characteristics are more universal, unique and permanent because they belong to a specific person*(20)*. Universality is reflected in the fact that humans universally share biometric characteristics, making it possible for biometric technology to be applied to every individual. Uniqueness reflects the distinctiveness and par-

ticularity of everyone's biometric characteristics, making precise identification possible. Permanence is based on the stability of an individual's biometric characteristics, making biometric characteristics matching possible via biometric technology. However, these properties of biometric characteristics also put themselves in a dangerous circumstance while enabling the application of biometric technology. Based on these properties, biometric characteristics are often considered the most reliable identification way and are directly associated with sensitive financial information, personal medical data, communication accounts and data, social identity, and other personal information as the most critical information. Once an individual's biometric characteristics are leaked, the associated privacy information may also be leaked, leaving the individual in a state of "zero privacy". Their universality expands the scope of privacy violations to a broader range of subjects; Their uniqueness makes attacks and frauds using leaked biometric characteristics more precise; Their permanence makes the consequences irreversible once leaked. At the same time, due to the potential for analysis and mining of biometric characteristics themselves and the development of biometric characteristics collection technology and other contemporary high-tech applications, this potential has become easier to realize. The possibility of theft of fingerprints, irises, facial features, and other biometric characteristics has increased. As can be seen, biometric technology puts new privacy represented by personal biometric characteristics at high risk.

For another, from the perspective of the connotation of the concept of privacy, biometric technology has resulted in the loss of privacy of the subject. According to the concept of privacy, privacy includes the ability to control one's information, the autonomy of individuals over information closely related to themselves, and self-determination rights, including freedom*(10)*. Biometric technology, on the other hand, separates the subject's biological characteristics from the subject, making biometric characteristics as privacy, which is no longer under the control of the subject. At the same time, the loss of anonymity of biometric characteristics also causes the subject to lose autonomy*(21)*. With the subject's permission, the one-time use of biometric characteristics can still be justified, but the storage and secondary use of biometric characteristics require further analysis. The purpose of storing individual biometric characteristics is often for secondary use (except for local storage for verification purposes), but whether secondary use is informed and consented to by the subject is key to whether it can be justified. In practice, few operators inform or obtain consent in advance when using subject information again.

Moreover, the purpose of secondary use may not necessarily be what was informed at the time of collection, and some even exchange or sell information. In addition, there are cases where biometric characteristics are obtained without the individual knowing. For example, privately installed surveillance cameras on streets are constantly capturing facial features, gait and even emotions of subjects every moment. Similar examples include real-time traffic images. Additionally, more and more applications use biometric technology, and biometric sensors are constantly increasing in resolution, accuracy, and capture precision*(12)*, making the situation even worse. For example, the widespread use of fingerprint and facial unlock functions on mobile phones and the development of healthy monitoring applications such as sleep monitoring, heart rate monitoring and pedometers have made access to sensitive medical and health data more easily. All these cases indicate that people's ownership and autonomy over their biological characteristics are greatly challenged. In this process, people are treated merely as means and lose their due dignity.

Where is the boundary of privacy protection in the application of biometric technology? Under what circumstances is the application of biometric technology justifiable? How to deal with the challenges it poses to privacy protection? In order to answer these questions, principled responses must be given.

4. Principled responses to privacy protection from biometric technology

The challenges of biometric technology to privacy protection fundamentally lie in the conflicts between ethical principles. The formulation of solu-

tions must be based on resolving these conflicts. Although the misuse of biometric technology may not necessarily be a good thing for protecting individual privacy, it has been widely used in some fields and brought great convenience in the current social development. At its root, the justification for using this technology comes from the utility derived from its use. Practical solutions can be developed only by addressing the relationship between privacy and utility.

4.1. The basic principles of the use of biometric technology

People take different positions on whether biometric technology should be used and whether privacy should be protected in its application. On the one hand, some advocate that a proactive relinquishment of privacy will determine the flourishing of personal and social virtue because people can freely share and use any information they desire in their own lives, which is the view of the "post-privacy movement"*(22)*. Others advocate the threat theory of biometric technology. They believe that biometric technology promotes and enhances the development of surveillance technology, which is inhumane, untrustworthy, and destructive to freedom*(23)*. The two opposing views are, in fact, extreme support for two ethical principles. The first upholds the principle of maximizing social benefit, intending to show that individual rights, represented by personal privacy, can be sacrificed to maximize social benefit.

In contrast, the second position upholds the principle of privacy protection and resists using biometric technology. Both positions are rather extreme, pitting the two principles diametrically against each other in an either/or manner, whereas in practice, our moral intuition tells us that both are needed. Suppose we relinquish the utility brought by biometric technology, such as convenience (avoiding queues, quickly answering questions, and timely access to information), efficiency (reducing costs and improving management efficiency), and spatial mobility (providing citizens with more convenient services, i.e., voting anywhere, services and movement of capital across borders through electronic services)*(23)*, it is difficult for society to develop and for human well-being to increase. If privacy is abandoned, human dignity and security are lost, and people are alienated into non-humanity. Human beings have pursued these ethical values throughout history and can co-exist under certain conditions.

In addition to the two principles mentioned above, we believe that an additional principle should be added — practical feasibility. Practical feasibility is such an important criterion because of the principle of "Ought Implies Can". In the *Critique of Practical Reason*, Kant says: "Pure geometry has postulates that are practical propositions, which, however, contain nothing more than the presupposition that one can do something if perhaps it were demanded that one should do it…"*(24)*. Human rationality and ability are limited, and moral law cannot require people to do what is impossible. This premise is one of the criteria used in formulating normative guidelines in many practical fields. Some scholars have further interpreted this: "When people use 'ought' to indicate action, the normative judgment only guides people in their actual activities to do a specific action when facing various available actions. The action indicated by the normative judgment must be something that people 'can' do; otherwise, it would force people to do something difficult and impossible to achieve its guiding purpose. For example, there is no obligation to require someone who cannot swim to jump into the water to save someone in danger"*(25)*. Similarly, when formulating ethical principles for applying biometric technology, the principle of practical feasibility should also be added; otherwise, even if criteria are established, they cannot be implemented in real life.

4.2. The hierarchy of different ethical principles

What is the relationship between different ethical principles? How should conflicts between basic ethical principles be resolved? These questions must be faced in responding to the challenges brought by biometric technology. Different perceptions of these questions have led to different positions, and we also present our position on this basis.

4.2.1. The position without conflict

On this question some people may challenge the validity of the question itself. Their stance is that there is no conflict between these ethical principles or that they are unaware of any such conflict.

One argument favoring biometric technology is that it can enhance privacy protection and is a "friend of privacy". The argument is based on the above-mentioned advantages compared to traditional identity recognition. Biometric technology provides stronger control over privacy protection, including defending personal identity, limiting access to information, and improving confidentiality*(26)*. Its application compensates for the weakness of traditional methods vulnerable to theft and falsification. Indeed, compared to traditional identity recognition, biometric technology is more reliable in recognition. However, it also entails more significant risks. As analyzed earlier, its universality, uniqueness, and permanence make the potential harm more severe than ever, even irreversible. Therefore, it is not reasonable to judge that there is no conflict between biometric technology and privacy protection based solely on the characteristics of biometric technology itself.

Another argument starts from the perspective that the characteristics recognized by biometric technology are non-personal and not owned by individuals. The question of who owns biometric characteristics after collection has been debated for a long time, especially for stored biometric characteristics. If we assume that once biometric characteristics are collected (even through legal procedures or informed consent), it is no longer owned by the collector but just digital information and has already been separated from the collector in its application. There is no issue of privacy infringement. However, is the premise that "stored biometric characteristics are not personal information" valid? Careful analysis of this premise reveals that the theoretical basis for supporting it is*(14,27)*: (a) stored biometric characteristics are meaningless digital numbers and not personally identifiable information; (b) biometric images cannot be reconstructed from biometric templates. For the first point, these stored "meaningless digital numbers" are extracted and transformed from individuals and are unique and can identify individuals*(14,28)*. For the second point, there are reports that biometric images can be reconstructed from templates*(14,29,30)*. Therefore, the view that "stored biometric characteristics are not personal information" is invalid. Thus, the position of no conflict based on this premise cannot stand.

4.2.2. The position of existing conflicts

In contrast to the position of without conflict, the position of existing conflicts is the view held by most people, acknowledging that there are conflicts between privacy protection and maximizing social benefits. The conflicts between the two can be intuitively aware of in real life. For example, when biometric technology is applied to public surveillance, it aims to maintain social order and combat crime. However, this means that citizens are constantly exposed to the surveillance of others. Fingerprint and face recognition payments also improve efficiency, save social and economic costs, and bring more significant social benefits while personal privacy has been transferred elsewhere. Within companies, attendance is checked through fingerprints and face recognition, ensuring the company's efficiency while controlling employees' privacy. These conflicts are inevitable, but in the face of conflicts, we cannot abandon either side. We cannot have social safety without personal privacy or disregard social interests only to defend individual rights.

4.2.2.1. Previous Solutions

Many acknowledge the existence of conflicts but do not provide a solution based on ethical principles. They only vaguely propose strengthening privacy protection in the technical field, reducing the probability of biometric characteristics being stolen, or preventing the abuse of biometric technology. However, this only increases the practical feasibility of privacy protection and does not explain how to choose when facing conflicts between privacy protection and maximizing social benefits. The problem cannot be fundamentally solved.

Similarly, providing answers based on specific situations cannot fundamentally solve the problem. The judgment of specific situations is also

based on a complete set of rules or guidelines, which must be based on rigid criteria. Moreover, on the one hand, judging every action specifically is not realistic. On the other hand, it is impossible to ensure that all factors and the consequences' pros and cons can be fully considered in a specific situation.

There is little discussion and weighing of basic ethical principles (first-order) in existing discussions. Instead, there is more discussion about formulating specific ethical governance principles (second-order) and operational guidelines (third-order). We believe that to solve the problem truly, and we must first respond from the basic ethical principles and weigh them against each other. Moreover, this kind of weighing must first carry out the ranking, weigh out priorities, and then further formulate specific ethical governance principles and operational guidelines based on the weighing of ethical principles.

4.2.2.2. The solution based on the hierarchy of ethical principles

Based on the above discussions, we believe that solving this problem requires fundamentally formulating the hierarchy of principles, that is, at the level of fundamental principles, should adhere to (i) the principle of practical feasibility; (ii) the principle of privacy protection (individual rights); (iii) the principle of maximizing social benefits. First, the principle of practical feasibility should be met, and on this basis, the principles of privacy protection and maximizing social benefits should be weighed. In weighing the two, the author believes that to achieve the principle of maximizing social benefits, satisfying the principle of individual privacy protection must be a prerequisite.

First and foremost, why do we need a hierarchy of principles? Primarily, from an etymological perspective, the Greek root of ethics is "ethos"*(31)*. Hegel pointed out that this word — ethos, especially in the Greek historian Herodotus, means "exquisite dwelling (vorzüglim Wohnung)"*(32)*. It means that it is in an "exquisite dwelling" that human beings develop natural and humane "habits" that enable them to lead a "good life"*(33)*. Therefore, ethics does not just focus on metaphysics but rather studies which choices are better in human practice. Only by comparing them can better choices be made. Secondly, from an individual perspective, developing any science and technology must benefit humans. Thirdly, from the perspective of the characteristics of science and technology, they all eventually move from the primitive and simple form to the form of integration and adaptation with ethics. Therefore, if biometric technology is to develop, it must adapt to ethics during its development process and balance the relationship between different ethical principles.

Next, how should we prioritize? As previously mentioned, formulating a guideline or a rule for a certain behavior implies that it can be achieved because "Ought Implies Can". If it is "impossible", then the formulation of such a guideline or rule is meaningless and merely empty talk. Whether it is the introduction of guidelines for applying biometric technology, the standardization of means for obtaining 'informed consent', or the stipulation of measures to strengthen privacy protection, they must first meet the principle of practical feasibility under current technological conditions.

After satisfying the principle of practical feasibility, the principle of privacy protection and the principle of maximizing social benefits are weighed. This paper argues that the principle of privacy protection takes precedence over the principle of maximizing social benefits. This view can be well defended from both deontological and utilitarian perspectives. From a deontological perspective, individual fundamental rights represented by privacy rights are basic human rights that represent the human free will and personal dignity. Their legitimacy derives from themselves and cannot be used as a means to an outer end. Individual fundamental rights can be arbitrarily violated if maximizing social benefits is prioritized. From a utilitarian perspective, privacy protection hinders information use and increases social costs (for example, making epidemiological research more difficult because, without informed consent from subjects, statistical data cannot be collected) *(23)*. However, the crisis of confidence caused by privacy violations also significantly increases social costs. Achieving so-called "maximum social

benefits" by violating privacy rights cannot achieve maximum utility. We cannot equate maximizing social benefits with maximizing economic benefits or with maximizing immediate benefits. Therefore, actions that promote maximum social benefits at the expense of privacy cannot be reasonably defended. From a rule utilitarian perspective, whether a specific action maximizes benefits cannot be used as a criterion for judging the justification of an action but should be indirectly linked to the principle of maximum utility through a set of rules*(34)*. An action is justifiable or defensible if and only if required by one or a set of principles that, if followed, will bring more significant benefits to society than any other principles*(34)*. As mentioned above, privacy protection may not directly promote maximum social benefits. Nevertheless, if everyone follows this rule, social trust will be guaranteed in the long run, and society can develop more stably. Biometric technology can make great development in its application due to gaining more trust in accessing information. Therefore, only by taking privacy protection as a prerequisite can true maximum social benefits be achieved.

The hierarchy of ethical principles is the most priority criterion. On this basis, specific ethical governance principles of the second-order are formulated, such as the principle of purpose explanation and permission during the data collection and the principle of informed consent and transparency during application. Furthermore, on top of that, make specific operational guidelines for the third-order, such as during the data collection: anyone asked to voluntarily submit a biometric identifier should (i) be fully aware of the potential risks; (ii) have the ability to understand the consequences of their actions; and (iii) consent to such actions in the absence of harm or threat*(35)*. The biggest challenge to this framework may come from social security. The traditional view may hold that law enforcement is an example of individual privacy rights giving way to public interests. In response to this point, we must first clarify that privacy protection does not mean that privacy cannot be used. Law enforcement's use of surveillance or biometric database does not necessarily result in privacy violations. It can be obtained through legal procedures. Compliance with legal procedures is a guarantee for protecting privacy. It is an example of maximizing social benefits based on privacy protection.

5. Conclusion

Through an in-depth analysis of the challenges of biometric technology to privacy protection, this paper concludes that the essence behind it is the conflicts between the two most fundamental ethical principles, namely maximizing social benefits and privacy protection. It provides a solution based on the hierarchy of ethical principles: biometric technology should be developed, but the premise of development is that ethical principles represented by the principle of privacy protection take precedence, and of course, these are based on the principle of practical feasibility. *The Personal Information Protection Law of the People's Republic of China* has come into effect, which echoes the ethical requirement of prioritizing privacy protection. Also, it provides a legal system guarantee for practical operations that can realize privacy protection. The solution based on the hierarchy of ethical principles proposed in this paper is to maximize social benefits further to ensure individual privacy rights, the premise of which is based on the principle of practical feasibility. It provides a solution to the ethical governance of biometric technology from the most basic principles and can be regarded as a first-order principle. It is the source for setting specific ethical governance principles and operational guidelines in the second and third orders and is also the basis for ensuring that biometric technology develops ethically. Based on this foundation, specific ethical governance principles in the second-order and operational guidelines in the third-order can be determined through Reflective equilibrium methods. At the same time, when formulating specific guidelines, attention must be paid to external regulations such as ethical review and legal regulation of biometric technology to achieve "good governance" in its use.

Conflict of interest

We claim no conflict of interest is associated with the "Challenges and Principled Responses to Privacy Protection from Biometric Technology in China" paper.

Acknowledgement:

This work was supported by the national key R&D project granted by the ministry of science and technology (Research on The Framework of Ethical Governance on Synthetic Biology, 2018YFA0902400).

References

1. Xuqi W. Identity deconstruction, ethical controversies and legal risks in AI face-swapping videos — the "ZAO" app as an example. *Southeast Communication* 2020; 3: 39-42.
2. Chunrun C. On technology expansion and social protection in the age of artificial intelligence — take "the first case of face recognition in China" as an example. *Administration and Law* 2021; 6: 95-108.
3. Yunying W. Reflections on the protection of personal information in face recognition. *National Judge College Law Journal* 2023; 2: 15-24.
4. He L. Be wary of the risk of facial recognition misuse. *Computer & Network* 2020; 46(16): 12.
5. Jing Y. Face recognition exposed to another security breach, unlocking 19 Android phones in 15 minutes with just a printer, *A4 paper and glasses frames* 2021 Jan 27. [Cited 2023 Apr 2] available from: URL: https://mp.weixin.qq.com/s?src=11&timestamp=1680534851&ver=4446&signature=2mk3aKJkM2FmeqfuMIPkbDwx8uTaXOs1MSKpJg5d3J36mbmVA9czTQPC0xkRgb09TwWp3vBOP-L5kFeUGhWCMkwe-YM0BJw1AaYHISM-eXxs1l6ngv8AId8n3VKzMZJE&new=1
6. ICSA. 1998 glossary of biometric terms. *Information Security Technical Report* 1998; 3(1): 98-108.
7. Pato J, Millett L. *Biometric recognition: challenges and opportunities*. Washington (DC): National Academies Press; 2010.
8. Snijder M. Biometrics, surveillance and privacy. *Joint Research Centre Science Hub* 2016.
9. Qichuan T, Runsheng Z. Survey on biometrics technology. *Application Research of Computers* 2009; 26(12): 4401-4406.
10. Kindt EJ. Biometric data, data protection and the right to privacy. In: Kindt EJ, eds. *Privacy and data protection issues of biometric applications: a comparative legal analysis*. Dordrecht: Springer Netherlands; 2013: 87-272.
11. De Hert P. Biometrics and the challenge to human rights in Europe. Need for regulation and regulatory distinctions. In: Campisi P, eds. *Security and Privacy in Biometrics*. London: Springer London; 2013: 369-413.
12. Al-Assam H, Kuseler T, Jassim S, et al. Privacy in biometric systems. In: Zeadally S, Badra M, eds. *Privacy in a digital, networked world: technologies, implications and solutions*. Cham: Springer International Publishing; 2015: 235-62.
13. Thomas FZ, Askar R, Renyu W, et al. Overview of biometric recognition technology. *Journal of Information Security Research* 2016; 2(01): 12-26.
14. Haiming H, Xiaomei Z. Biometrics applications: an overview of ethical issues. *Science and Society* 2018; 8(03): 49-59.
15. Woodward JD. The law and the use of biometrics. In: Jain AK, Flynn P, Ross AA, eds. *Handbook of biometrics*. Boston (MA): Springer US; 2008: 357-79.
16. Parker RB. A definition of privacy. *Rutgers University Law Review* 1973; 27(2): 275-297.
17. North-Samardzic A. Biometric technology and ethics: beyond security applications. *Journal of Business Ethics* 2020; 167(3): 433-450.
18. Bélanger F, Crossler RE. Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly* 2011; 35(4): 1017-1041.
19. Xinbao Z. From privacy to personal information: theories and institutional arrangements for remeasuring interests Institutional Arrangements. *China Legal Science* 2015; 3: 38-59.
20. Mordini E, Petrini C. Ethical and social implications of biometric identification technology. *Annali dell'Istituto Superiore di Sanità* 2007; 43(1): 5-11.
21. Campisi P. Security and privacy in biometrics: towards a holistic approach. In: Campisi P, eds. *Security and Privacy in Biometrics*. London: Springer London; 2013: 1-23.
22. Dratwa J. Ethics of security and surveillance technologies: *European Group on Ethics Opinion Report* 2014.
23. Sutrop M. Ethical issues in governing biometric technologies. In: Kumar A, Zhang D, eds. *Ethics and policy of biometrics*. Heidelberg: Springer Berlin; 2010: 102-114.

24. Kant I. *Critique of practical reason*. Indianapolis (IN): Hackett Publishing; 2002.
25. Song Y. "Ought imply can" and obligation. *Journal of Beijing Normal University (Social Science)* 2014; 2:102-108.
26. Orlans NM, Higgins PT, Woodward JD. *Biometrics*. New York (NY): McGraw-Hill/Osborne; 2003.
27. Mordini E. Ethics and policy of biometrics. In: Tistarelli M, Li SZ, Chellappa R, eds. *Handbook of remote biometrics: for surveillance and security*. London: Springer London; 2009: 293-309.
28. Woo RB. Challenges posed by biometric technology on data privacy protection and the way forward. In: Kumar, A., Zhang, D. eds. *Ethics and policy of biometrics*. Heidelberg: Springer Berlin; 2010: 1-6.
29. IAPC, Cavoukian A. *Fingerprint biometrics: address privacy before deployment*. Ontario: Information and Privacy Commissioner of Ontario; 2008.
30. Feng J, Jain AK. FM model based fingerprint reconstruction from minutiae template. In: Tistarelli, M, Nixon, MS, eds. *Advances in biometrics*. Heidelberg: Springer Berlin; 2009: 544-553.
31. Walker P, Lovat T. Should we be talking about ethics or about morals? *Ethics & Behavior*. 2017; 27(5): 436-444.
32. Hegel GWF. *Georg wilhelm friedrich hegel grundlinien der philosophie des rechts oder naturrecht und staatswissenschaft im grundrisse*. Frankfurt: Suhrkamp Verlag; 1972.
33. Anqing D. The tension structure of "morality" and "ethicality" in Kant's practical philosophy: critique of Habermas' again: on the relationship between morality and ethicality. *Philosophical Analysis* 2020; 11(03): 132-145.
34. Lian C. *Keywords in ethics*. Beijing: Beijing Normal University Publishing Group; 2007.
35. Alterman A. "A piece of yourself": ethical issues in biometric identification. *Ethics and Information Technology*. 2003; 5(3): 139-150.

Received: April 4, 2023
Accepted: May 3, 2023