2022

Assessing Legal Protection of Biometric Data in China: Gaps, Principles, and Policy Recommendations

Qian Li

Jianyu Zhou

Jennifer S. Stevenson

JOURNAL OF LEGAL MEDICINE
2022, VOL. 42, NOS. 3–4, 123–141
https://doi.org/10.1080/01947648.2024.2307624

Taylor & Francis
Taylor & Francis Group

Assessing Legal Protection of Biometric Data in China: Gaps, Principles, and Policy Recommendations

Qian Li[*], Jianyu Zhou[†], and Jennifer S. Stevenson[#]

ABSTRACT

The legal protection of biometric data is becoming an increasingly important issue in the information society. China attaches importance to the legal protection of biometric data. Over the past decades, the rapid development of digital technology has profoundly influenced Chinese information society. However, digital technology may also trigger substantial risks. In this article, we provide an in-depth examination of existing Chinese laws protecting biometric data. We explore general laws and facial recognition laws, administrative regulations, sector-based rules, judicial interpretations, regulatory documents, policy documents, and (draft) national standards. We find gaps in laws in China. Building on this analysis, we elaborate on five principles for the legal protection of biometric data: (1) legality, propriety, and necessity; (2) integrity; (3) purpose; (4) minimization; and (5) controllability. We provide three policy recommendations for the legal protection of biometric data: (1) sufficiently considering the purpose of the collection of biometric data, (2) creating controllable mechanisms, and (3) implementing regulatory compliance programs.

Table of contents

[*] School of Law, The Institute for Chinese Legal Modernization Studies, Nanjing Normal University, Nanjing, China E-mail: qianli@nnu.edu.cn
[†] Health Law Department, Weifang Medical University, Weifang, China
[‡] School of Law, St. Mary's University, San Antonio, Texas

I. INTRODUCTION

The legal protection of biometric data is becoming an increasingly important issue globally for both governments and the private sector. Singapore's Personal Data Protection Commission has observed the importance of legal protection of biometric data, focusing on key considerations in implementing security cameras and biometric recognition systems.[1] This is significant because a series of biometric data security incidents have impacted the public. In 2019, an artificial intelligence company in China focused on security was exposed to a large-scale data breach including ID card information, facial recognition images, etc.[2] In 2021, the personal data, including biometric data, of more than half a billion Facebook Inc. users reemerged online for free.[3] In 2022, Central Florida Inpatient Medicine acknowledged a data security breach including Social Security numbers, full names, financial account numbers, home addresses, medical diagnoses, etc.[4]

[1] *See* PERSONAL DATA PROTECTION COMMISSION & SECURITY ASSOCIATION SINGAPORE, GUIDE ON RESPONSIBLE USE OF BIOMETRIC DATA IN SECURITY APPLICATIONS (2022), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-toBiometric_17May2022.ashx?la=en.

[2] *See* Wang Lin & Xi Sun Ji, *AI Security Companies Were Exposed to Data Leakage and Sounded the Alarm on Face Recognition Security*, CCTV.com (Feb. 26, 2019, 6:45 AM), https://news.cctv.com/2019/02/26/ARTIpBI3zrVbQxjZ78yraD83190226.shtml.

[3] *See* Bloomberg, *Facebook Data on 533 Million Users Reemerge Online for Free*, L.A. Times (Apr. 3, 2021, 1:40 PM), https://www.latimes.com/business/story/2021-04-03/facebook-data-hack.

[4] *See Central Florida Inpatient Medicine Breach*, ID Strong (Sept. 16, 2022), https://www.idstrong.com/sentinel/central-florida-inpatient-medicine-breach/.

Countries around the world have responded to biometric data security concerns. More than a hundred countries have enacted laws and regulations to protect biometric data. Major laws and regulations enacted include the Illinois Biometric Information Privacy Act,[5] the California Consumer Privacy Act,[6] the Washington Privacy Act,[7] the Deepfakes Report Act of 2019,[8] the General Data Protection Regulation,[9] and the European Commission Artificial Intelligence Act.[10]

China also attaches importance to the legal protection of biometric data. In China, biometric data is defined as personal data obtained by technical processing of the physical, biological, or behavioral characteristics of a natural person that can identify that natural person alone or in combination with other data, including personal facial recognition features, iris recognition, fingerprints, genes, voice, gait, palm prints, auricles, eye scans, etc.[11]

How to adequately protect the above types of biometric data is one of the most important current issues in China. Over the past decades, the rapid development of digital technology has profoundly influenced Chinese information society. However, digital technology may also trigger substantial risks. For example, with the wide use of digital technology, the leakage of biometric data, the lack of authority, and deep fakes may bring about social problems because biometric data are highly associated with personal identity and cannot be easily changed.[12] More specifically, the wide use of facial recognition technology has led to personal data leakages.[13] Prior to 2021, China had enacted laws and regulations in response to these

[5] 740 Ill. Comp. Stat. Ann. 14/10 (West 2008).

[6] California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100-199 (West 2019).

[7] Washington Privacy Act, S.B. 5376, 66th Leg., Reg. Sess. (Wash. 2019).

[8] Deepfake Report Act of 2019, S. 2065, 116th Cong. (2019).

[9] 2016 O.J. (L. 119/1) 679.

[10] EUR. PARL. DOC. (52021PC0206) 206 (Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts).

[11] *See* xìnxī ānquán jìshù gèrén xìnxī ānquán guīfàn (信息安全技术 个人信息安全规范) [Information Security Technology—Personal Information (PI) Security Specification] (promulgated by State Administration for Market Regulation, Oct. 11, 2021, effective May 1, 2022) GB/T 40660—2021, Oct. 11, 2021, at 5, https://www.chinesestandard.net/PDF.aspx/GBT40660-2021.

[12] *See* SHĒNGWÙ SHÍBIÉ YǏNSĪ BǍOHÙ YÁNJIŪ BÀOGÀO (生物識別隱私保護研究報告) [Biometric Privacy Protection Research Report], CAICT (中國信通院) [CAICT], http://www.caict.ac.cn/kxyj/qwfb/ztbg/202010/P020201028364732231494.pdf (last visited Dec. 21, 2023).

[13] *See* Rénliǎnshíbié Shíshī Guānchá: Jìshùlànyòng,Yìngyòng Mángqū, 70% Yònghù Dānxīn Shùjù Xièlòu (人臉識別實施觀察:技術濫用,應用盲區,70%使用者擔心數據洩露) [Observation of Facial Recognition Implementation: Abuse of Technology, Blind Spots of Applications, 70% of Users Concerned about Data Breaches], nándū réngōngzhìnéng lúnlǐ yánjiūzǔ (南都人工智慧倫理研究組) [Nandu Artificial Intelligence Ethics Research Group] (Jan. 7, 2020, 4:29 PM), http://cbdio.com/BigData/2020-01/07/content_6154002.htm.

problems of data protection.[14] Nevertheless, these laws and regulations have not adequately addressed the ever-increasing issues facing biometric data. In August 2021, China enacted the Personal Information Protection Law (PIPL) to establish ground rules for the processing of biometric data.

The PIPL is one of the key laws protecting biometric data.[15] The PIPL protects biometric data by combining other fundamental laws and regulations. The PIPL describes what constitutes the legal protection of biometric data and guides individuals in taking proper processing and preventive measures because it established which types of biometric data processing is illegal and therefore banned.

These functions raise the question of how biometric data are processed in China in both the public and private sectors. The use of facial recognition technology involves massive amounts of biometric data. Current Chinese rules governing the use of facial recognition in the public sector generally encourage greater use and integration of the technology, leaving out important concerns regarding how to strike a balance between individual interests and public needs.[16] These concerns are being taken into consideration in China, because China has proposed existing laws to provide comprehensive protection of biometric data. Yet, as technical advancements have outpaced legal actions,[17] it is unclear how effectively these existing laws will regulate biometric data. In Section II, we provide an in-depth examination of existing Chinese laws protecting biometric data, using facial recognition laws as a case study. In Section III, we find three gaps in laws related to facial recognition technology. In Section IV, we elaborate on five

[14] These laws and regulations in China mainly include: the Decision on Strengthening Network Information Security by the NPC Standing Committee (promulgated by the Nat'l People's Cong. Standing Comm., Dec. 28, 2012, effective Dec. 28, 2012), China Copyright and Media: The Law and Policy of Media in China; Regulations Regarding Telecom and Internet Users' Personal Information Protection by the Ministry of Industry and Information Technology (promulgated by Ministry of Industry and Information Technology, June 28, 2013, effective Sept. 1, 2013), DIGICHINA, July 16, 2013, https://digichina.stanford.edu/work/telecommunications-and-internet-personal-user-data-protection-regulations/; and the Biosecurity Law (promulgated by Nat'l People's Cong. Standing Comm., Oct. 17, 2020, effective Apr. 15, 2021), The Nat'l People's Cong. of China, Oct. 17, 2020, http://en.npc.gov.cn.cdurl.cn/2020-10/17/c_703568.htm; etc.

[15] It is commonly acknowledged that fundamental laws in China are the Cybersecurity Law (2016), the Biosecurity Law (2020), the Civil Code (2020), the Personal Information Protection Law (2021), and the Data Security Law (2021). *See* Cybersecurity Law of China (promulgated by Nat'l People's Cong. Standing Comm., Nov. 7, 2016, effective June 1, 2017), Cyberspace Admin. of China, Nov. 7, 2016, http://www.cac.gov.cn/2016-11/07/c_1119867116_3.htm; *see id.*, Biosecurity Law; Civil Code of China (promulgated by Nat'l People's Cong. Standing Comm., May 28, 2020, effective Jan. 1, 2021), The State Council of China, Dec. 31, 2020, https://english.www.gov.cn/archive/lawsregulations/202012/31/content_WS5fedad98c6d0f72576943005.html; Personal Information Protection Law of China (promulgated by Nat'l People's Cong. Standing Comm., Aug. 20, 2021, effective Nov. 1, 2021), China Briefing, Aug. 24, 2021, https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/; Data Security Law of China (promulgated by Nat'l People's Cong. Standing Comm., June 10, 2021, effective Sept. 1, 2021) The Nat'l People's Cong. of China, June 10, 2021, http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html.

[16] Yan Luo & Rui Guo, *Facial Recognition in China: Current Status, Comparative Approach and the Road Ahead*, 25 U. Pa. J.L. Soc. Change 153, 158 (2021).

[17] Iria Giuffrida, *Liability for AI Decision-Making: Some Legal and Ethical Considerations*, 88 Fordham L. Rev. 439, 440 (2019).

principles for the legal protection of biometric data. In Section , we provide three policy recommendations for the legal protection of biometric data. A brief conclusion follows.

II. EXISTING CHINESE LAWS GOVERNING BIOMETRIC DATA

Over the past few years, China has witnessed massive processing of biometric data, especially facial recognition data. Facial recognition is deployed to identify citizens for law enforcement purposes, such as performing identity verification at airports, train stations, or specific public areas, and for commercial purposes to enhance business operations' efficiency.[18] We argue that facial recognition is one of the most common methods for biometric data processing in China, and China needs to ensure that biometric data are processed legitimately and reasonably. In a broad sense, all processing of biometric data in China may be measured as to whether it is legitimate and reasonable. Keeping this in mind, we intend to explore how China treats biometric data under its existing laws.

A. General Laws and Facial Recognition Laws

The main general laws and facial recognition laws regarding the protection of biometric data are the Cybersecurity Law, the Biosecurity Law, the Civil Code, the PIPL, and the Data Security Law. Each of them uses different methods for protecting biometric data.

The Cybersecurity Law focuses on network information security. Articles 40 to 45 of the Cybersecurity Law require network operators, individuals, organizations, and departments that assume cybersecurity supervision to effectively protect personal information, including biometric data. For example, Article 41 of the Cybersecurity Law forbids network operators from illegally processing biometric data, stating that "network operators shall not collect personal information irrelevant to the services provided by them, shall not collect or use personal information in violation of the provisions of any law or administrative regulation or the agreement of both parties and shall dispose of personal information preserved by them under the provisions of laws and administrative regulations and agreements with users."[19]

The Biosecurity Law strengthens human genetic resource information security.[20] It is widely acknowledged that genetic data are an important type of biometric data. The Biosecurity Law establishes a general principle for handling human genetic resource information, stating that "the

[18] *See* Luo & Guo, *supra* note 16, 159-62.

[19] *See* Cybersecurity Law of China, *supra* note 15, art. 41.

[20] *See* Biosecurity Law, *supra* note 14, art. 85(8).

collection, preservation, use, and outbound supply of China's human genetic resources shall conform to ethical principles and be without harm to public health, national security, or public interest."[21]

The Civil Code aims to provide full remedies for infringements of privacy rights and personal information. Biometric data are associated with individuals' privacy rights and personal information. The Civil Code offers two paths for protection of biometric data, stating that "private information in personal information shall be governed by the provisions on privacy rights; where there are no provisions, the provisions on the protection of personal information shall apply."[22]

The PIPL provides important rules for the processing of biometric data. Article 26 of the PIPL sets several restrictions on overprocessing of biometric data, stating that "the installation of image collection or personal identification equipment in public places shall be necessary for maintaining public security and comply with relevant provisions issued by the state, and conspicuous signs shall be erected."[23] It also states that "the collected personal images and identification information can only be used to maintain public security, and shall not be used for other purposes, except with the separate consent of individuals."[24] In addition, the PIPL uniquely includes a section containing general rules and specific rules for the processing of sensitive personal information, including biometric data.[25]

The Data Security Law imposes data security protection obligations for specific data subjects. These data security protection obligations are increasingly vital to the legal protection of biometric data because purely relying on the subjects' control over processing of their biometric data is insufficient to safeguard the interest of individuals subject to automated decision making. Moreover, a categorized and hierarchical data protection system is necessary to lay a solid foundation for protecting biometric data.[26]

B. Administrative Regulations

In China's digital society, it is increasingly necessary to protect biometric data by drafting related administrative regulations. The most notable example is the Regulation on the Administration of Credit Investigation Industry. The administrative regulation aims to protect biometric data in

[21] *See id.*, art 55.

[22] *See* Civil Code of China, *supra* note 15, art. 1034.

[23] *See* Personal Information Protection Law of China, *supra* note 15, art. 26.

[24] *Id.*

[25] *See* Personal Information Protection Law of China, *supra* note 15, ch. 2, sec. 2.

[26] *See* Data Security Law of China, *supra* note 15, art. 21.

the context of credit investigations. Article 14 of this administrative regulation states that “credit investigation institutions may not collect information about the income, deposit, negotiable securities, commercial insurance, real property or taxes of individuals unless they have expressly informed the individuals concerned of the possible adverse consequences that may be brought along with the provision of such information and have obtained their written consent.”[27] Thus, in principle, credit investigation institutions are prohibited from collecting biometric data such as personal religious beliefs, facial recognition data, etc.[28]

C. Sector-Based Rules

Sector-based rules are being created for specific and detailed issues regarding the processing of biometric data. In China, one of the most important sector-based rules is the Regulations on the Administration of Network Data Security (Draft). Under that rule, the processing of biometric data can only occur after conducting a risk assessment on its necessity and security and shall not be used as the only method of personal identification as a way to force individuals to consent to the collection of their biometric data.[29] This is a fundamental principle for the processing of biometric data.

D. Judicial Interpretations

On June 8, 2021, the Supreme Court People’s Court issued a judicial interpretation of facial recognition technology. The judicial interpretation points out that facial information comprises biometric data as stipulated by Article 1034 of the Civil Code.[30] It also defines what constitutes valid consent for processing facial information.[31] Additionally, it enumerates several exemptions from civil liability, such as processing facial information in

[27] *See* Regulation on the Administration of Credit Investigation Industry (promulgated by the State Council, Dec. 26, 2012, effective Mar. 15, 2013), art. 14, The People’s Bank of China, Jan. 21, 2013, http://www.pbc.gov.cn/en/3688253/3689006/3858830/index.html.

[28] *See* Zhongshao Gao, *“Multi-Layered” Legal Norms Protecting Facial Recognition Data* (in Chinese), Prosecutor Daily (Sept. 8, 2019), https://www.spp.gov.cn/spp/llyj/202109/t20210908_528821.shtml.

[29] *See* Notice of the Cyberspace Administration of China on the “Regulations on the Management of Network Data Security (Draft for Solicitation of Comments)” for Public Solicitation of Comments, art. 25, Cyberspace Admin. of China, Nov. 14, 2021, http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm.

[30] *See* zuìgāorénmínfǎyuàn guānyú shěnlǐ shǐyòng rénliǎnshíbié jìshù chǔlǐ gèrénxìnxī xiāngguān mínshì ànjiàn shìyòng fǎlǜ ruògān wèntí de guiding (最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定) [Provisions of the Supreme People’s Court on Several Issues Concerning the Application of Law in the Trial of Civil Cases Relating to Processing of Personal Information by Using Facial Recognition Technology], art. 1, Libr. Of Cong. (Sup. People’s Ct. Jun. 8, 2021) (China), https://www.loc.gov/item/global-legal-monitor/2021-08-15/china-supreme-peoples-court-issues-judicial-interpretation-against-misuse-of-facial-recognition-technology/.

[31] *See id.* at art. 4.

response to a public health emergency, protecting a natural person's life and health and property under emergent circumstances, or using facial recognition technology in public places under the relevant regulations to maintain public security.[32] Apart from this judicial interpretation, there are several judicial interpretations concerning criminal liability for processing personal information, including biometric data.

E. Regulatory Documents

Several regulatory documents are associated with the processing of biometric data. The most notable example is the Guidance for Internet Personal Information Security Protection. The regulatory document requires that Chinese citizens' sensitive data, such as race, ethnicity, political views, religious beliefs, etc., should not be collected or processed on a large scale.[33] These sensitive data include specific types of biometric data. Other regulatory documents relate to the processing of biometric data under the context of mobile internet applications, such as the scope of necessary personal information required for common types of mobile applications (apps) involving specific biometric data.[34]

F. Policy Documents

A policy document is a more specific guideline to regulate the processing of biometric data; for example, the Measures for the Determination of the Collection and Use of Personal Information by Apps in Violation of Laws and Regulations. This policy document emphasizes that the app should notify the user of its purpose, and the purpose for collecting sensitive personal information involving biometric data should be clear and easy to understand.[35]

[32] *See* Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law, *supra* note 30, art. 5.

[33] *Supra* note 11.

[34] *See* Provisions on the Scope of Necessary Personal Information Required for Common Types of Mobile Internet Applications (promulgated by Cyberspace Administration of China, the Ministry of Industry and Information Technology, and the Ministry of Public Security, and the State Administration for Market Regulation, Mar. 12, 2021, effective May 1. 2021), China Network Information Network, Mar. 22, 2021, http://www.cac.gov.cn/2021-03/22/c_1617990997054277.htm.

[35] *See* Measures for Determination of Violations of Laws and Regulations in APPs' Collection and Use of Personal Information (Draft for the Solicitation of Comments), sec. 2.3, China Law Translate, May 7, 2019, https://www.chinalawtranslate.com/en/measures-for-determination-of-violations-of-laws-and-regulations-in-apps-collection-and-use-of-personal-information-draft-for-the-solicitation-of-comments/.

G. (Draft) National Standards

Creating (draft) national standards concerning the processing of biometric data is an important hallmark under Chinese existing laws. There are two main (draft) national standards. The first is the draft Information Security Technology—Requirements for Security of Face Recognition Data ("Draft Standard"). The Draft Standard focuses on security requirements for the processing of facial recognition data when data controllers carry out "facial verification" and "facial identification."[36] The characteristics of these security requirements involve the minimization, voluntary nature, and necessity of using facial recognition and technology-based recovery measures. The Draft Standard also includes security requirements for facial recognition data from the perspective of the whole life cycle, including collecting, storing, using, delegated processing, sharing, transferring, and publicly disclosing facial recognition data.[37] These designs aim to use technical measures to safeguard the dynamic security of the whole life cycle of facial recognition data processing. The second is the Information Security Technology—Personal Information Security Specification (GB/T 35273-2020). This national standard enumerates specific kinds of biometric data, such as medication records, in the area of personal physical and physiological data.[38]

III. GAPS IN CHINESE LAWS REGULATING FACIAL RECOGNITION DATA

According to the above existing laws, biometric data can be used to identify a natural person.[39] In the context of processing the unique biological characteristics of a natural person, there are gaps in laws regarding the legal protection of biometric data. Biometric data, a product of the digital age, are easily stolen, resulting in personal data security risks due to the invisibility of the collection, processing, and subsequent illegal transactions of biometric data.[40] At present, gaps in laws in China allow the collection of personal data that may lead to the risk of harm, unlawful processing leading to the risk of losing personal control, and the abuse of information leading to actual damages or harm.

[36] See Provisions on the Security Management of the Application of Facial Recognition Technology (Provisional), art. 4, Cyberspace Administration of China, Aug. 8, 2023, https://mp.weixin.qq.com/s/ZbsL8qfU0fXF031ZUomE3A.

[37] *See id.* at art. 6.

[38] *Supra* note 11.

[39] *See* Qi Zhang & Dongmei Xiao, *The Judicial Application Dilemma and Outlet of Biometric Information Definition in China* (in Chinese), 42(7) Libr. Trib. 53 (2022).

[40] *See* Xiuwen Gu & Bo Zhang, *Research on Legal Regulation of Personal Biometric Information Application Risk* (in Chinese), 187(4) Soc. Sci. Heilongjiang 76 (2021).

Thus, we need to explain the relationship between the above three gaps. The first gap is the massive collection leading to the risk of harm, infringing upon personal rights and interests. The second gap is unlawful processing leading to the risk of losing personal control, which does not include massive collection. In addition, losing personal control reveals that subjects fail to exercise the right to information self-determination rather than merely personal rights and interests, such as the right to the name, portrait, privacy, etc. The third gap is the abuse of biometric data leading to actual damages or harm.

A. Massive Collection Leading to the Undetectable Risk of Harm

The collection of biometric data is ubiquitous in a digital society. For example, Alipay and WeChat may give price discounts when collecting users' facial data through "scan face payment." If individuals do not give their consent, the unauthorized collection of biometric data will violate their property rights.[41] In addition, the massive collection of biometric data may directly lead to infringement of the right to the name, portrait, and privacy, which further leads to infringement of personal rights and interests based on personal freedom and personal dignity, because biometric data have the characteristic of strong personal specificity.[42]

An undetectable risk of harm means is understood as follows: the risk of harm cannot be perceived in time and the subject cannot take relief measures in time, leading to an expansion of the risk of harm, especially in the context of network communication.[43] Because biometric technology works in real time, the conversion from language to text is completed almost synchronously; thus, users are often unaware of the existence of biometric technology.[44] In other words, the subject may not perceive the risk of harm caused by the massive collection of biometric data.

B. Unlawful Processing Leading to the Risk of Losing Personal Control

Unlawful processing leading to the risk of losing personal control is the second gap in the law. Biometric recognition technology, which is regarded as high-tech, has a wide range of applications in our digital society. However, unlawful processing by biometric recognition technology is

[41] *See* Xianquan Liu & Yimin Lu, *Construction and Perfection of Criminal Law Protection of Biometric Information* (in Chinese), 117(1) J. Soochow U. (Phil.& Soc. Sci. Edition) 62 (2022).

[42] *See id.*

[43] *See* Liping Gu, *From Identity Recognition to Body Manipulation: Research on Privacy Protection in Intelligent Biometric Technology* (in Chinese), 64(5) J. Shanghai Normal U. (Phil.& Soc. Sci. Edition) 11 (2021).

[44] *See* Kunru Yan & Dan Liu, *Involvement of Technology and Its Ethical Protocol Based on Biometric Identification Technology* (in Chinese), 19(1) J. Ne. U. (Soc. Sci.) 4 (2017).

common because legal regulation cannot keep up with the rapid development of technology.[45] The first facial recognition case, which has attracted widespread attention, involves privacy infringement and personal data leakage risk caused by biometric technology.[46] The abuse of biometric technology involving the unauthorized use and disclosure of personal data may infringe on a subject's privacy.[47] In a broad sense, almost all unlawful processing may lead to the risk of losing personal control.

The leakage of large-scale personal biometric data and fake videos of public figures losing personal control may cause public panic and social disorder.[48] For example, users' static and dynamic facial data, fingerprints, iris scans, gait, and other biometric data improperly leaked by a "ZAO" software in China may be exposed to property losses.[49] This example shows that the leakage of personal biometric data is likely to trigger substantial risks or losses.

C. Abuse Leading to Actual Damages or Harm

The abuse of biometric data will likely cause actual damage or harm. The development and wide use of digital technology and algorithms are likely to increase actual personal damage or harm. For example, biometric data, such as facial data, fingerprints, iris scans, and gait, collected by specific digital machines, could be abused by automated decision making, causing actual damages or harm to personal rights and property rights.

In addition, abuse of biometric data can cause actual damages or harm to public security and national security. For example, if suspects use biometric data to impersonate a financial industry officer, make false videos, release false information, and publicly spread it on the internet, such false information may make securities, bonds, and the foreign exchange market volatile, creating a chain reaction, seriously affecting the stability of financial markets.[50] In this view, the chain reaction includes investors' blind investments leading to investment losses, damage to the reputation of

[45] *See* Liping Gu, *Identity Recognition and Replication: Privacy Protection in the Application of Intelligent Biometrics* (in Chinese), 50(4) J. Soc. Sci. of Hunan Normal U. 126 (2021).

[46] *See* 郭兵与杭州野生动物世界有限公司服务合同涉人脸识别纠纷(guō bīng v hángzhōu yěshēng dòngwùshìjiè) [Bing Guo v. Hangzhou Wildlife World Co., Ltd.], China Laws Portal (Hangzhou Fuyang District People's Court Nov. 20, 2020) (China).

[47] *See* Nenggao He & Jingkun Wang, *Legal Risks and Rules of Biometric Technology Application: A Case Study of Bing Guo* (in Chinese), 258(6) Just. China 44 (2021).

[48] *See* Yang Yu, *On the Regulatory Structure of the Application Risk of Personal Biometric Information* (in Chinese), 29(6) Admin. L. Rev. 103 (2021).

[49] *See* Guorui Sun, *Will a "ZAO" Face-Swapping Software Confront Copyright Risks?* (in Chinese), People.cn (September 6, 2019), http://ip.people.com.cn/n1/2019/0906/c179663-31340892.html.

[50] *See* Gu & Zhang, *supra* note 40, at 63.

financial industries, undue influence on financial markets that seriously affects their stability, etc.

IV. RECOMMENDATIONS FOR PRINCIPLES

Given the existing laws and gaps in laws, we argue that five main principles can be applied to the protection of biometric data: (1) legality, propriety, and necessity; (2) integrity; (3) purpose; (4) minimization; and (5) controllability. There are three facets we need to clarify.

First, these five principles were chosen because they are stipulated in China's PIPL. The PIPL stipulates that personal information shall be processed under the principles of lawfulness, legitimacy, necessity, and good faith and shall not be processed in a way that is misleading, fraudulent, or coercive.[51]

Second, academic proposals for principles are advisory and not mandatory. Article 5 of the PIPL is used to regulate the processing of personal information. It is necessary to expand its role for use in regulating biometric data processing.

Third, relationships among these five principles have two dimensions. On one hand, legality, propriety, necessity, and integrity reveal respect for the willingness of individuals. The purpose principle, minimization principle, and controllability principles overlap. For example, Article 6 of the PIPL emphasizes that the collection of personal information shall be limited to the minimum extent necessary to achieve the purpose of processing, and personal information shall not be collected excessively.[52] Article 6 may be regarded as an overlap between the purpose principle and the minimization principle. On the other hand, the necessity principle is enriched by the minimization principle. The necessity principle aims to strike a balance between the processing of information and the protection of information, requiring information processors to follow the minimization principle and take the approach that has the least impact on individual rights and interests.

A. Legality, Propriety, and Necessity

Legality means that biometric data processing must comply with laws and regulations. Propriety means that biometric data processing should be reasonable and should not be contrary to public order and good morals.[53] Necessity refers to a proper limit to biometric data processing and is

[51] Personal Information Protection Law of China, *supra* note 15, art. 5.

[52] *See id.*, art. 6.

[53] *See* Civil Code of China, *supra* note 15, art. 8.

necessary for data processors or data controllers. These principles promote risk prevention and harm reduction.[54] Legality, propriety, and necessity are vital to the existing laws. Biometric data processing shall strictly follow this principle to strengthen the protection of biometric data.

B. Integrity

Integrity is increasingly important in the context of civil activities. Article 7 of the Civil Code stipulates that "the parties to civil legal relations shall conduct civil activities under the principle of good faith, adhere to honesty, and fulfill their promises."[55] As for the processing of biometric data, the integrity principle means that the biometric identification system can implement data integrity protection through access control to prevent unauthorized access or through the use of integrity checking using encryption.[56] For example, if a data controller fails to take vigorous measures to safeguard biometric data security, it will be necessary to implement the integrity principle to evaluate his behavior. Ke Xu helpfully proposes that specific processing of personal information without fraud or manipulation could be regarded as an integrity mechanism supplementing the obligation of the personal information processor.[57] If data controllers handle biometric data without fraud or manipulation, they are following the integrity principle.

C. Purpose

The purpose principle is included in Article 6 of the PIPL and involves three elements: specificity, reasonableness, and direct relevance.[58] The specificity element means that the purpose for biometric data processing cannot be broad. For example, subjects should not be required to consent to the collection of their biometric data by a business function that they did not apply for or use by bundling the business functions of the product or service.[59] The reasonableness element means that the processing of biometric data shall comply with the laws and public order and good morals. The direct relevance element means that the processing of biometric data shall

[54] Shi Hui Qiu & Ming Hu, *Legislative Moves on Biosecurity in China*, 40 Biotechnology L. Rep. 30 (2021).

[55] *See* Civil Code of China, *supra* note 15, art. 7.

[56] *See* Yong Zhang, *Legal Protection of Personal Bioinformation Security: A Case Study of Face Recognition* (in Chinese), 42(5) Jiangxi Social Sciences 161 (2021).

[57] *See* Ke Xu, *The Integrity Principle: A Trust Path to Balance Personal Information Protection and Utilization* (in Chinese), 34(5) Peking U. L. J. 1143, 1145-50 (2022).

[58] *See* Personal Information Protection Law of China, *supra* note 15, art. 6.

[59] *Supra* note 11.

meet its purpose. According to Article 28 of the PIPL,[60] processors may not process biometric data unless there are specific purposes and sufficient necessity and strict protection measures are taken. In a word, the three elements emphasize the purpose itself and its direct relevance with the processing of biometric data.

D. Minimization

Minimization refers to a situation where the processing of biometric data shall have the minimum impact on the rights and interests of data subjects, and the collection of biometric data shall be limited to the minimum scope necessary to achieve the processing purpose and shall not be excessive.[61] Data processors should take specific measures to mitigate risks to the rights and interests of subjects. The collection of biometric data should be narrow. The frequency of automatic collection of biometric data should be the minimum frequency necessary to achieve the business functions of the product or service. Also, the amount of indirect access to biometric data should be the minimum amount necessary to fulfill the business functions of the product or service.[62]

E. Controllability

The controllability principle refers to processors taking responsibility for their biometric data processing activities, including necessary measures to guarantee the security of the biometric data they process.[63] The traditional data security paradigm includes confidentiality, integrity, and availability, which specialists often call the "CIA triad."[64] For security in the data flow, the traditional data security paradigm has difficulty meeting the security requirements, and a new data security paradigm in which a controllability principle is inherent should be introduced.[65] The controllability principle requires data processors to fulfill many obligations to safeguard biometric data, including, but not limited to, developing internal management rules and operating procedures; taking corresponding technical security measures, such as encryption and de-identification; developing and organizing

[60] *See* Personal Information Protection Law of China, *supra* note 15, art. 28.

[61] *See id.*, art. 6.

[62] *Supra* note 11.

[63] *See* Personal Information Protection Law of China, *supra* note 15, art. 9.

[64] *See* Kristen E. Eichensehr, *Giving Up on Cybersecurity*, 64 UCLA L. Rev. Discourse 320, 324 (2016).

[65] *See* Jin Rui Liu, *The Reform of Data Security Paradigm and Its Legislative Development* (in Chinese), 43(1) Glob. L. Rev. 1, 10-11 (2021).

the implementation of emergency plans for biometric data security incidents; etc.[66]

V. POLICY RECOMMENDATIONS

In this section, based on the principles outlined above, we will provide several policy recommendations for the legal protection of biometric data.

A. Sufficiently Considering the Purpose of the Collection of Biometric Data

We argue that data processors need to sufficiently consider the purpose of the collection of biometric data when collecting biometric data. Data processors usually include individuals, companies, public institutions, and governments. Given the PIPL's stipulations and realistic risks of the massive collection of biometric data often triggered by companies, we analyze how companies may sufficiently consider the purpose of the collection of biometric data. We argue that all types of companies may sufficiently consider the purpose of the collection of biometric data when they serve as data processors. It is worth noting that different types of companies may take different steps.

First, companies providing important internet platform services, which have a large number of users and whose business models are complex, may implement feasible privacy-preserving biometric schemes. Some privacy-preserving biometric schemes (PPBSs) to protect biometric data that contain individuals' privacy information have been developed in recent years, including biometric encryption-based schemes, cancelable biometric based schemes, multimodal and hybrid-based schemes, and secure computation-based schemes.[67] These PPBSs may take the proper purpose of the collection of biometric data into consideration. For example, if a sports corporation is interested in developing apps for fitness, it would consider the reasonable purpose of the collection of biometric data when implementing specific PPBSs. This is because users usually store their data locally and thus their devices need to be secured to prevent unauthorized access.[68]

Second, companies that present apps may provide publicly available certification standards. In China, communication apps, video apps, entertainment apps, etc., need to collect biometric data. Companies who present these apps may provide publicly available national or international certification standards to demonstrate that the specific app has the necessary

[66] *See* Personal Information Protection Law of China, *supra* note 15, art. 51.

[67] *See* Iynkaran Natgunanathan et al., *Protection of Privacy in Biometric Data*, (4) IEEE Access 880, 880 (2016).

[68] *See* Claudia Diaz, Omer Tene, & Seda Gurses, *Hero or Villain: The Data Controller in Privacy Law and Technologies*, 74(6) Ohio St. L. J. 923, 949 (2013).

safeguards for the purpose of the collection of biometric data,[69] of whatever type, to facilitate the legal, proper, and necessary collection of biometric data.

Third, companies that need to handle specific individuals' biometric data may strictly obey the purpose rules for the collection of biometric data. When companies need to handle specific individuals' biometric data, they should show that the purpose is legitimate and there is a direct relevance for the collection.

B. Creating Controllable Mechanisms

Creating controllable mechanisms for responding to unlawful processing is helpful to reduce the risk of losing personal control. The practical challenges in the processing of biometric data are, in some ways, attributable to changes in technology.[70] Addressing technology that is constantly evolving has long been a critical challenge for data protection laws.[71] Against that background, collectives involving governments, companies, social organizations, and individuals need to create controllable mechanisms to regulate the automatic processing of biometric data. When it comes to the relationship between governments, companies, social organizations, and individuals, we argue that (1) governments play fundamental roles, (2) companies are obligated to take steps to safeguard the security of processing biometric data, and (3) social organizations and individuals are encouraged to create controllable mechanisms. Relying entirely on companies, social organizations, and individuals to create controllable mechanisms will fall short of adequately protecting subjects' biometric data. There is certainly a need to consider government's role. Governments are responsible for supervising companies' controllable mechanisms when companies provide important internet platform services, have a large number of users, and have complex business models.

First, controllable mechanisms need a multi-governance model to control the risk across the full life cycle of biometric data processing. Initially, a multi-governance model was used during European integration.[72] However, multi-governance models are now implemented in other fields, such as environmental governance and data governance. A multi-governance model

[69] *See* Xixue Shang, *China's Position and Institutional Approach to the Commercial Application of Biometric Information—Given the Comparative Evaluation of European and American Law Models* (in Chinese), 40(2) Jiangxi Soc. Sci. 200 (2020).

[70] *See* Muge Fazlioglu, *Beyond the Nature of Data: Obstacles to Protection Sensitive Information in the European Union and the United States*, 46(2) Fordham Urban L. J. 271, 302 (2019).

[71] *See* Spiros Simitis, *Privacy—An Endless Debate?*, 98(6) Calif. L. Rev. 1989, 2000 (2010).

[72] *See* Liesbet Hooghe & Gary Marks, *Multi-Level Governance and European Integration*, 5(11) EIoP 1, 4-5 (2001).

could also be utilized in the processing of biometric data. The government may create controllable mechanisms and guidelines for enforcing controllable rules. Companies providing important internet platform services, that have a large number of users, and whose business models are complex may release tailored operating manuals on the controllable mechanisms when they collect biometric data. Social organizations may reinforce compliance assessments and certification services in the processing of biometric data. Individuals may keep their biometric data in mind and have increased awareness of biometric data processing.[73]

Second, imposing controllable duties on biometric technology is increasingly important. The fact that biometric data can be faked, however, is not a complete indictment of the technology.[74] The real problem is not that biometrics are subject to fraud or error but rather our conviction nonetheless in its accuracy.[75] From this view, it is vital to impose controllable duties on biometric technology to ensure its accuracy. Data processors may make explicit controllable steps across the full life cycle of biometric data processing. For example, layered controllable techniques are needed for biometric data storage when it is exposed to different substantial risks of storage. Data processors may also keep track of the processing of biometric data to evaluate the substantial risks that will exist. For example, anyone who accesses, modifies, and downloads biometric data needs to be identifiable, so that data processors may pursue the responsibility for triggering substantial risks.[76]

C. Implementing Regulatory Compliance Programs

Regulatory compliance programs aim to prevent potential biometric data abuse. We argue that different types of companies are responsible for regulatory compliance programs. Three main scenarios are as follows.

First, companies that handle biometric data reaching quantities determined by the state cybersecurity and information department need to build regulatory compliance offices to have overall responsibility for biometric data use. Regulatory compliance offices aim to supervise biometric data use, conduct risk assessments, and communicate with government information supervisors and industry associations.[77] Supervising biometric data use

[73] *See* Qian Li, *Fraud Internet Flow Needing a Multi-Governance Model* (in Chinese), People's Ct. Daily (Dec. 30, 2021), https://www.chinacourt.org/article/detail/2021/12/id/6461808.shtml.

[74] Robin Feldman, *Considerations on the Emerging Implementation of Biometric Technology*, 25 Hastings Comm. & Ent. L. J. 653, 665 (2003).

[75] *Id.*

[76] *See* Hui Qiang Xing, Legal Regulation of Face Recognition (in Chinese), Inst. of Rule of L., China Univ. Pol. Sci. L. (June 14, 2021), http://fzzfyjy.cupl.edu.cn/info/1035/13047.htm.

[77] *See* Yu, *supra* note 48.

means that the regulatory compliance office needs to take effective measures to take charge of all activities involving biometric data use. Regulatory office risk assessments often include the purposes and methods of biometric data use, categories of biometric data, the impacts on individuals' rights and interests, and the limiting of potential risks by taking corresponding security technical measures such as encryption and de-identification.[78] Alerting government information supervisors and industry associations when potential biometric data abuse happens is necessary.[79] In addition, government information supervisors may interview the legal representatives or primary persons in charge of companies that handle biometric data reaching quantities determined by the state cybersecurity and information department if they find there are relatively large risks in biometric data use or if any biometric data security incident occurs.[80]

Second, companies that develop products and manage business processes may hold an idea of "privacy by design." Privacy by design is a process for embedding good privacy practices into the design specifications of technologies, business practices, and physical infrastructures.[81] We contend that it is crucial to embed good privacy practices into biometric data use. Companies can introduce relevant subjects' preferences and expectations of biometric data use and record the process of biometric data use to let data subjects know how their biometric data will be used.[82] In this sense, privacy by design strengthens both personal control of biometric data and the security of biometric data use.

Third, for-profit private companies may reduce related legal risks by implementing regulatory compliance programs. In China, for-profit private companies will face related legal risks when they use subjects' biometric data without implementing regulatory compliance programs. Thus, for-profit private companies effectively implementing regulatory compliance programs may be exempt from specific legal punishments. Apart from civil punishments stipulated in the Civil Code and administrative punishments stipulated in the PIPL, specific legal punishments mainly are criminal punishments. For example, if a data collection company implements a regulatory compliance program to identify persons who abuse personal facial recognition data, the data collection company would not be subject to pun-

[78] *See* Personal Information Protection Law of China, *supra* note 15, art. 56.

[79] See *id.* at art. 57.

[80] See *id.* at art. 64.

[81] *Privacy by Design*, Australian Government, https://www.oaic.gov.au/privacy/privacy-for-organisations/privacy-by-design (last visited Dec. 22, 2023).

[82] *See* Wei Fan, *Reconstruction of the Path of Personal Information Protection in the Era of Big Data* (in Chinese), Inst. of Rule of L., China Univ. Pol. Sci. L. (June 25, 2021), http://fzzfyjy.cupl.edu.cn/info/1035/13097.htm.

ishment for the crime of infringement on citizens' personal information.[83] Implementing regulatory compliance programs would reduce criminal risk because abusing personal facial recognition data is essentially identity fraud.[84]

CONCLUSION

The legal protection of biometric data in China is a critical issue. China protects biometric data through general laws and facial recognition laws, administrative regulations, sector-based rules, judicial interpretations, regulatory documents, policy documents, and (draft) national standards. In a digital society, there are three gaps in Chinese laws, such as massive collection leading to the undetectable risk of harm, unlawful processing leading to the risk of losing personal control, and abuse leading to actual damages or harm. In response to these gaps, we analyze five main principles: (1) legality, propriety, and necessity; (2) integrity; (3) purpose; (4) minimization; and (5) controllability. Then we provide three main policy recommendations for the legal protection of biometric data: (1) sufficiently considering the purpose of the collection of biometric data, (2) creating controllable mechanisms, and (3) implementing regulatory compliance programs.

DISCLOSURE STATEMENT

The authors declare that they have no conflict of interest.

FUNDING

The article is supported by the Major Program of the National Fund of Philosophy and Social Science of China "Research on the Construction of Criminal Security Risk Prevention System in Digital Economy" (21&ZD210) and the General Project of Philosophy and Social Science Research in Colleges and Universities in Jiangsu "Research on the Idea and Path of Criminal Regulation of Flow Fraud Driven by Algorithm" (2022SJYB0243).

[83] *See* Criminal Law of China (promulgated by Nat'l People's Cong. Standing Comm., July 1, 1979, rev. Dec. 28, 2002, effective Oct. 1, 1997), art. 253, Congressional Executive Commission on China, Jan. 15, 2013, https://www.cecc.gov/resources/legal-provisions/criminal-law-of-the-peoples-republic-of-china#2%20Chapter%20XI.

[84] *See* Huai Sheng Li, *On the Criminal Responsibility about the Abuse of Personal Biometric Information—Taking Artificial Intelligence "Deepfake" as an Example* (in Chinese), 38 Trib. Pol. Sci. and L. 144, 151-52 (2020).