

CHINA'S EMERGING LEGAL REGIME FOR PRIVACY AND PERSONAL INFORMATION PROTECTION

Chengxin Peng*

Guosong Shao**

Wentong Zheng***

Table of Contents

I.INTRODUCTION	3
II.THE CONSTITUTIONAL FOUNDATION	5
III.THE CIVIL CODE	8
A. Right to Privacy	9
B. Protection of Personal Information	11
C. Distinctions Between Privacy and Personal Information	14
1. Conceptual Overlaps	14
2. Similarities and Differences in the Attributes of Rights and Interests	15
3. Differences in the Exercise of Rights and Interests	16
IV.THE PERSONAL INFORMATION PROTECTION LAW	17
A. The Legislative Background of the PIPL	17
B. The Relationship Between the PIPL and the Civil Code	18
C. Main Provisions of the PIPL	19
1. Rules on Processing of Personal Information	19
2. Rules on Cross-Border Transmission of Personal Information 21	
3. Personal Information Rights and Obligations	22
4. Regulatory Agency for Personal Information Protection	23
5. Legal Liability	24
V.REMAINING ISSUES	24

* Chengxin Peng, Dean & Professor, KoGuan School of Law, Shanghai Jiao Tong University

** Guosong Shao, Director & Professor, The Center for Media and Public Affairs, Shanghai Jiao Tong University.

*** Wentong Zheng (corresponding author), Professor, University of Florida Levin College of Law.

A. The Dichotomy of Privacy and Personal Information Protection	24
B. The Interface of Personal Information Processing Rules with Multiple Processing Scenarios	26
C. Different Obligations for Different Information Processors	27
D. “Separate Consent” and “Security Assessment” for Cross-Border Data Flows	28
E. Administrative Penalties and Discretions	29
F. Limited Practical Impact	30
VI.CONCLUSIONS.....	30

CHINA'S EMERGING LEGAL REGIME FOR PRIVACY AND PERSONAL INFORMATION PROTECTION

Chengxin Peng

Guosong Shao

Wentong Zheng

Abstract

China plays an increasingly important role in shaping the global legal landscape on privacy and data protection issues. This article discusses China's emerging legal regime for the protection of privacy and personal information. The article identifies three pillars of this legal regime: China's Constitution, which lays the foundation for protecting privacy and personal information, and the Civil Code and the Personal Information Protection Law, two recent laws that implement the Constitution's requirements. The article explores the intricacies of the three pillars in light of recent case law developments while referencing the legal standards in other jurisdictions such as the European Union's General Data Protection Regulation. Finally, the article discusses the remaining issues in China's legal regime that need to be further clarified or resolved.

Key Words: Privacy; Personal Information; China; Constitution; Civil Code; Personal Information Protection Law

I. INTRODUCTION

Home to the largest population and the largest number of internet users in the world,¹ China plays an important role in the global regulation of privacy and personal information. Although the legal protection of privacy and personal information is rooted in China's Constitution,² efforts to establish a legal framework for privacy and personal information protection in China did not start in earnest until the early 2000s.³ Such efforts led to the enactment of a series of privacy-related laws, regulations, judicial interpretations, and

¹ As of February 2022, China ranked first among the countries with the most internet users in the world. China had 1.02 billion internet users, more than triple the number of third-ranked United States. See Statista, Countries With the Highest Number of Internet Users as of February 2022, <https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/#:~:text=Countries%20with%20the%20highest%20number%20of%20internet%20users%202022&text=As%20of%20February%202022%2C%20China,over%20307%20million%20internet%20users>.

² See *infra* Part I.

³ The Tort Law of 2009, for the first time, formally included the right to privacy as one of protected civil rights. See Zhonghua Renmin Gongheguo Qinquan Zeren Fa (中华人民共和国侵权责任法) [The Tort Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 26, 2009, effective Jul. 1, 2010), art. 2, http://www.gov.cn/flfg/2009-12/26/cOontent_1497435.htm.

industrial standards,⁴ culminating in the incorporation of privacy and personal information protection in China's Civil Code in 2020⁵ and the adoption of China's first comprehensive personal information protection legislation, the Personal Information Protection Law ("PIPL") in 2021.⁶ Today, China has become one of the most active players in digital privacy regulation,⁷ with frequent agency rulemaking and enforcement actions targeting privacy violations on digital platforms.⁸ Thanks to the sheer size of China's economy and its important role in the global industries, what transpires in China in the realm of

⁴ See Quanguo Renmin Daibiao Dahui Changwu Weiyuanhui Guanyu Jiaqiang Wangluo Xinxin Baohu de Jueding (全国人民代表大会常务委员会关于加强网络信息保护的決定) [The Decision of the Standing Committee of the National People's Congress on Strengthening the Protection of Online Information] (promulgated by the Standing Comm. Nat'l Cong. Dec. 28, 2012); Xiaofeizhe Quanyi Baohu Fa (消费者权益保护法) [The Law on the Protection of Consumer Rights and Interests] (promulgated by the Standing Comm. Nat'l People's Cong. Oct. 31, 1993, amended Aug. 27, 2009 and Oct. 25, 2013); Wangluo Anquan Fa (网络安全法) [The Cybersecurity Law] (promulgated by the Standing Comm. Nat'l People's Cong. Nov. 7, 2016, effective Jun. 1, 2017); Minfa Zongze (民法总则) [The General Provisions of the Civil Law] (promulgated by the Standing Comm. Nat'l People's Cong. Mar. 15, 2017, effective Oct. 1, 2017); Dianzi Shangwu Fa (电子商务法) [The E-Commerce Law] (promulgated by the Standing Comm. Nat'l People's Cong. Aug. 31, 2018, effective Jan. 1, 2019); Xingfa Xiuzheng An (Qi) (刑法修正案(七)) [Amendment (VII) to the Criminal Law] (promulgated by the Standing Comm. Nat'l People's Cong. Feb. 28, 2009, effective Feb. 28, 2009); Xingfa Xiuzheng An (Jiu) (刑法修正案(九)) [Amendment (IX) to the Criminal Law] (promulgated by the Standing Comm. Nat'l People's Cong. Aug. 29, 2015, effective Nov. 1, 2015); Zuigao Renmin Fayuan Guanyu Shenli Liyong Xinxin Wangluo Qinhai Ren Shen Quanyi Minshi Jiufen Anjian Shiyong Falu Ruogan Wenti de Guiding (最高人民法院关于审理利用信息网络侵害人身权益民事纠纷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 Cases Involving Civil Disputes Over Infringements Upon Personal Rights and Interests through Information Networks] (2014); Zuigao Renmin Fayuan Zuigao Renmin Jiancha Yuan Guanyu Banli Qinfan Gongmin Geren Xinxin Xingshi Anjian Shiyong Falv Ruogan Wenti de Jieshi (最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释) [Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Infringing on Citizens' Personal Information] (2017); Zhengxin Jigou Guanli Banfa (征信机构管理办法) [Regulation on the Administration of Credit Investigation Industry] (2013); Geren Jongrong Xinxin Baohu Jishu Guifan (个人金融信息保护技术规范) [Technical Standards for the Protection of Personal Financial Information] (2020); Xinxin Anquan Jishu Jiankang Yiliao Shuju Anquan Zhinan (信息安全技术健康医疗数据安全指南) [Guidelines on Information Security Technology for Health Care Information Security] (2021); Renlei Yichuan Ziyuan Guanli Tiaoli (人类遗传资源管理条例) [Measures on the Management of Human Genetic Resources] (2019).

⁵ Minfa Dian (民法典) [Civil Code] (promulgated by the Nat'l People's Cong. May 28, 2020, effective Jan. 1, 2021) (hereinafter referred to as the "Civil Code"), arts. 1032–39, <http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml> (Chinalawinfo).

⁶ Geren Xinxin Baohu Fa (个人信息保护法) [The Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong. Aug. 20, 2021, effective Nov. 11, 2021) (hereinafter referred to as the "PIPL"), <http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml> (Chinalawinfo).

⁷ Alexandra S. Levine, "Deeply Alarmed": China Now Ahead of U.S. on Privacy Law, POLITICO CHINA WATCHER (July 8, 2021), <https://www.politico.com/newsletters/politico-china-watcher/2021/07/08/deeply-alarmed-china-now-ahead-of-us-on-privacy-law-493497> (citing Glenn Gerstell, former National Security Agency general counsel).

⁸ See Josh Horwitz, *China Passes New Personal Data Privacy Law, to Take Effect Nov. 1*, REUTERS (Aug. 20, 2021), <https://www.reuters.com/world/china/china-passes-new-personal-data-privacy-law-take-effect-nov-1-2021-08-20/>.

privacy and personal information protection affects not only the livelihoods of Chinese citizens but also the business models of multinational corporations.⁹

As important as China is for privacy and personal information protection, navigating the country's complex legal rules on this issue is no easy matter. This article undertakes to examine the three pillars of privacy and personal information protection in China: the Constitution, the Civil Code, and the PIPL. China's Constitution provides the overarching foundation for China's legal regime on privacy and personal information. The Civil Code elevates the protection of privacy and personal information from that afforded under decentralized and fragmented rules to systematic legislative protection. The PIPL serves as the basic law on personal information protection, setting out rules on the processing of personal information, the rights of information owners in information processing activities, the obligations and responsibilities of information processors, and the cross-border transfer of personal information.¹⁰

This article first explains the constitutional basis of privacy and personal information protection in China and then illustrates the two most important laws in this field, namely, the Civil Code and the PIPL. After this, this article tries to assess the whole system of privacy and personal information protection, pointing out its characteristics well as problems.

II. THE CONSTITUTIONAL FOUNDATION

Unlike under U.S. law, where the U.S. Constitution recognizes a right to privacy against unreasonable government searches and seizures,¹¹ the right to privacy has not been developed in the constitutional sense under Chinese law as an autonomous right. Nonetheless, the protection of privacy and personal information is embedded in China's Constitution. To elaborate, Article 33 of China's Constitution requires that "the State respects and protects human rights."¹² Article 37 specifies that "the personal freedom of citizens is

⁹ For instance, on November 1, 2021, when China's new Personal Data Privacy Law took effect, Yahoo shut down the few remaining services it was operating in China, citing "an increasingly challenging business and legal environment." Matt Burgess, *Ignore China's New Data Privacy Law at Your Peril*, *Wired* (Nov. 5, 2021), <https://www.wired.com/story/china-personal-data-law-pipl/>.

¹⁰ Relatedly, the Data Security Law, enacted in June 2021, imposes data security obligations on entities engaged in data processing activities, and provides legislative support for standardizing data processing activities, protecting data security, promoting data development and utilization, and protecting the legal rights of individuals and organizations. *See Shuju Anquan Fa (数据安全法)* [Data Security Law] (promulgated by the Standing Comm. Nat'l People's Cong. June 10, 2021, effective Sept. 1, 2021), <http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml>) (Chinalawinfo).

¹¹ *See* U.S. CONST. amend. IV. The U.S. Supreme Court has interpreted the Fourth Amendment to protect people from warrantless searches of places or seizures of persons or objects in which they have a reasonable expectation of privacy. *See, e.g., Katz v. United States*, 389 U.S. 347, 351–52 (1967).

¹² *See* ZHONGHUA RENMIN GONGHEGUO XIANFA (中华人民共和国宪法) [THE CONSTITUTION OF THE PEOPLE'S REPUBLIC OF CHINA] (promulgated by the Nat'l People's Cong. Dec. 4, 1982, amended Mar. 11, 2018), art. 33, http://www.xinhuanet.com/politics/2018lh/2018-03/22/c_1122572202.htm (hereinafter Constitution).

inviolable.”¹³ Article 38 states that “the personal dignity of citizens is inviolable.”¹⁴ Articles 39 and 40 stipulate the “inviolability of the home” and “the freedom and secrecy of correspondence” respectively.¹⁵ All these provisions indicate that the Constitution intends to protect individual freedom and dignity.

The more difficult question, however, is how to connect the general personality right in the Constitution to the right to privacy and personal information under civil laws. One way of making this connection is to examine the nature of the Constitution itself. China’s Constitution has never been a law that merely restrains the public power of the state; it is also a law that restrains private individuals and entities. Under the Constitution, the state assumes the responsibility of protecting the personal dignity of citizens from infringements by third parties.¹⁶ This places China’s Constitution in the “horizontal effect” model of constitutional law, which regulates relationships among private individuals as well as relationships between governments and private individuals.¹⁷

The second way of connecting the general personality right in the Constitution to the right to privacy and personal information is through the traditional method of statutory interpretation. The two main provisions in China’s Constitution that are closely related to the right to privacy and personal information are the “human rights clause” and the “personal dignity clause,” both of which provide the basic values and norms underlying China’s privacy and personal information protection laws.

The “human rights clause” in Article 33 of the Constitution recognizes and protects “human rights.”¹⁸ These rights are considered to include unenumerated fundamental rights or general freedom.¹⁹ The necessity to recognize these unenumerated fundamental rights in the human rights clause lies in the demand for constitutional texts to remain open to interpretation, given the inherent tensions between legal texts and social change in countries operating under codified statutes.²⁰ These unenumerated fundamental rights provide ample space for construing the human rights protected under the Constitution to include the right to privacy and personal information since the latter has the attribute of protecting human rights.

The “personal dignity clause” in Article 38 of the Constitution provides that the personal dignity of citizens is inviolable, and insults, defamation, and false

¹³ *Id.* art. 37.

¹⁴ *Id.* art. 38.

¹⁵ *Id.* arts. 39 & 40.

¹⁶ See ZHANG XIANG (张翔), *JIBEN QUANLI DE GUIFAN JIANGOU* (基本权利的规范建构) [THE NORMATIVE CONSTRUCTION OF FUNDAMENTAL RIGHTS] 120–21 (2008).

¹⁷ For discussions of the “horizontal effect” model, see Stephen Gardbaum, *The “Horizontal Effect” of Constitutional Rights*, 102 MICH. L. REV. 387, 388 (2003).

¹⁸ See XIANFA, *supra* note 12, art. 33, para. 3 (“The State respects and protects human rights.”).

¹⁹ See Li Zhongxia (李忠夏), *Shuzi Shidai Yinsiquan de Xianfa Jiangou* (数字时代隐私权的宪法建构) [The Constitutional Construction of the Right to Privacy in the Digital Age], 3 HUADONG ZHENGFA DAXUE XUEBAO (华东政法大学学报) [J. EAST CHINA UNIV. POLITICAL SCIENCE & L.], 46 (2021).

²⁰ *Id.*

accusations against citizens by any means are prohibited.²¹ The first sentence of this clause sets out the right to personal dignity in a general sense, and the second sentence enumerates specific instances of violations of personal dignity. One might be tempted to conclude that, from a technical point of view, this enumeration restricts the general right of personality in civil law to “insults, defamation, and false accusations” and excludes other elements of the right of personality. This interpretation of the personal dignity clause, however, lacks a sufficient basis. On the one hand, it is true that the Constitution is the fundamental law of the highest order, and the relationship between the Constitution and the sectoral laws should be analyzed as a legal system in which the Constitution plays a leading role. This is why, regardless of the legal level of protecting privacy and personal information, the ultimate purpose of such protection can be traced to the constitutional value of maintaining fundamental personal freedom and dignity. On the other hand, one shall not neglect the interpretative function of the Constitution. The personal dignity clause states that “insulting, defaming, or falsely accusing citizens using any methods is prohibited.”²² The term “any” in the clause can be interpreted in an expanded manner for purposes of protecting the personal dignity of citizens.²³ Since the purpose of a normative system of fundamental rights is to establish the protection of fundamental rights of the individual, an expansive interpretation consistent with the purpose of protection is permissible in principle. The term “any” can contextually extend the protection of personal dignity to the prohibition of infringement of the personal dignity of citizens in the form of criminal offenses, as well as infringement of the constitutional right of personal dignity in the form of infringement of the general civil right of personality, thus extending the scope of application of Article 38.

Through such interpretations, the fundamental human right enshrined in the Constitution is operationalized in a legal system of protecting human dignity at the level of ordinary laws, and the constitutional right of personal dignity is implemented in ordinary statutes. This implementation can be seen in the legislative language. Under the PIPL, for example, the addition of the phrase “in accordance with the Constitution” to Article 1 in the final draft of the law is not accidental. Some may think that this phrase is unnecessary because whether or not this phrase exists, interpretations of ordinary statutes are required to be carried out in accordance with the Constitution. However, the phrase “in accordance with the Constitution” does reveal the legislator’s consideration that the PIPL is a law based on the Constitution. To some extent, this provision confirms that the protection of personal information is derived from the unenumerated fundamental rights in the Constitution, which are of the highest importance

²¹ See XIANFA art. 38, (2018).

²² *Id.*

²³ See Zheng Xianjun (郑贤君), *Xianfa “Renge Zunyan” Tiaokuan de Guifan Diwei zhi Bian (宪法“人格尊严”条款的规范地位之辩)* [The Debate on the Normative Status of the “Human Dignity” Clause of the Constitution], 2 ZHONGGUO FAXUE (中国法学) [CHINA LEGAL SCIENCE] 87, 87–88 (2012).

in the legal hierarchy but lack practical applications. Therefore, although privacy and personal information rights are derived from the Constitution, the protection of such rights will have to be implemented by statutes such as the PIPL. The value of freedom and personal dignity in the Constitution is thus realized.²⁴

Indeed, the phrase “in accordance with the Constitution” has a normative meaning—that is, many fundamental rights of different forms all emanate from the personal dignity clause in Article 38 of the Constitution, which should be interpreted as the core source of legal rights protected by the PIPL. Although the Constitution cannot be used directly as a legal basis, constitutional interpretations can be carried out in a way to link the Constitution to the legal norms specified in statutes such as the PIPL. While being rooted in the constitutional text, interpretations of the Constitution shall adapt to changing times and enable the construction of a diversified system of personal information protection. Conversely, the norms of personal information protection should reflect the basic value of personal dignity protected by the Constitution and realize the “radiant effect of basic rights” so as to ultimately achieve the purpose of protecting personal dignity.²⁵

III. THE CIVIL CODE

The second pillar of China’s legal regime for privacy and personal information protection is China’s Civil Code, which provides comprehensive—yet bifurcated—protection for the two subject matters. To elucidate the rather complex legal principles established in the Civil Code, we start with a high-profile legal case, the *WeChat Reading* case, which was decided under the Civil Code.

²⁶

The basic facts of the *WeChat Reading* case are as follows. WeChat Reading is a mobile application that allows users to read and comment on books. WeChat is a mobile application that allows users to add friends and engage in instant communications. The plaintiff discovered that WeChat Reading displayed the contacts from his WeChat as the ones following the same books as he was because WeChat shared his contacts with WeChat Reading. Moreover, WeChat Reading shared the names of the books the plaintiff was reading and his comments on the books with the plaintiff’s contacts from WeChat. The

²⁴ However, this has also given rise to a debate on the relationship between the PIPL and the Civil Code, that is, whether it is one of parallelism or one of special law versus general law. See Wang Xixin (王锡锌) & Peng Chun (彭鑫), *Geren Xinxi Baohu Falü Tixi de Xianfa Jichu* (个人信息保护法律体系的宪法基础) [*The Constitutional Basis of the Legal System of Personal Information Protection*], 3 QINGHUA FAXUE (清华法学) [TSINGHUA UNIVERSITY L. J.] 6, 7 (2021).

²⁵ Zhang Xiang (张翔), *Geren Xinxi Quan de Xianfa (Xue) Zhengcheng—Jiyu dui Qufen Baohu Lun he Zhipeiquan Lun de Fansi* (个人信息权的宪法(学)证成——基于对区分保护论和支配权论的反思) [*The Constitutional Foundation of Personal Information Rights—Rethinking Differentiated Protections and Disposal Rights*], 1 HUANQIU FALÜ PINGLUN (环球法律评论) [GLOBAL L. REV.] 53, 53–58 (2022).

²⁶ See *Tengxun Keji (Shenzhen) Youxian Gongsi Deng Wangluo Qinquan Zeren Jiufen Yishen Panjueshu* (腾讯科技(深圳)有限公司等网络侵权责任纠纷一审判决书) [Huang v. Tengxun Keji Co., Ltd.], (2019)京0491民初16142号 (Beijing Internet Ct.2019).

plaintiff alleged that WeChat violated his right to privacy and personal information, and demanded the cessation of violations and apologies from the defendant companies owned by Tencent.²⁷

In its ruling, the Beijing Internet Court held that information about a user's contacts and reading activities on WeChat is personal, but not private. Since the personal information gathered from WeChat Reading has a close connection with personality rights, migrating personal information from WeChat to WeChat Reading and displaying this information to friends not followed by users runs a high risk of infringing upon users' rights and interests of personal information. Therefore, prominent notifications should be provided to users to ensure users' full knowledge of the scope of information usage and its risks. By collecting users' contacts from WeChat and disclosing users' reading activities to contacts not followed by users without users' consent, WeChat Reading violated users' rights and interests of personal information. But since the information about users' reading activities does not rise to the level of private information, such information sharing by WeChat Reading did not violate users' right to privacy. Similarly, WeChat Reading violated users' rights and interests of personal information, not their right to privacy, when it automatically followed users' contacts from WeChat, enabling those contacts to gain access to information about users' reading activities on WeChat Reading.²⁸

As a result, the court ordered the defendant companies to stop sharing information about the plaintiff's reading activities on WeChat Reading with contacts from his WeChat account. The court also ordered the defendant companies to issue an apology to the plaintiff and to pay for the plaintiff's expenses for notarizing documents in the amount of RMB 6600 yuan (about US \$1000).²⁹

It is rather clear from the WeChat Reading case that the Civil Code treats the right to privacy and the rights and interests of personal information differently. Below, this article offers an analysis of the contents of the two rights and interests and their overlaps.

A. *Right to Privacy*

Prior to the enactment of the Civil Code, the right to privacy in China was initially protected through the right to reputation, was then protected as a personality right with limitations, and was finally recognized in 2009 in the Tort Law as a specific personality right with an independent status.³⁰ In recent years,

²⁷ See *Su Weixin Dushu An Xuanpan*: Zidong Guanzhu Moren Zhanshi Dushu Xinxi Qinfan Geren Xinxi Quanyi (诉微信读书案宣判：自动关注、默认展示读书信息侵犯个人信息权益) [Judgment in the WeChat Reading Case: Automatic Following, Displaying Information About Users' Reading Activities Violate Rights and Interests of Personal Information], SOHU NEWS (July 30, 2020), https://www.sohu.com/a/410610123_161795, last visited June 23, 2023.

²⁸ See *id.*

²⁹ See *id.*

³⁰ The General Provisions of the Civil Law of 2017 provided for the right to reputation, in which the invasion of privacy was considered a tort of reputation. See *Zhonghua Renmin Gongheguo Minfa Zongze* (中

with the development of information technology, the legal protection of personal information received more attention, and the Civil Code passed in 2020 differentiated the rights and interests of personal information from the right to privacy and protected both as separate legal rights or interests. The distinction between the right to privacy and the rights and interests of personal information indicates that China adopts a narrow interpretation of the right to privacy, and the right to privacy is the bottom line in dealing with issues of personal information.³¹

The Tort Law of 2009 and the General Provisions of Civil Law of 2017 included the right to privacy as a specific personality right but did not define the scope of privacy. The Civil Code supplemented these laws in terms of protecting the right to privacy. Paragraph 1 of Article 1032 of the Civil Code specifies that the holders of the right to privacy are natural persons, and do not include legal persons and unincorporated organizations.³² This is because the right to privacy is a personality right, and the purpose of protecting the right to privacy is to safeguard the personal dignity and the personal freedom of natural persons. The most important characteristic of the right of personality is that it is not a property right. Since the private information of an enterprise legal person is inextricably linked to its economic interests, it is regarded as the property of the enterprise.

Paragraph 2 of Article 1032 sets out the scope of the right to privacy protected under civil law. Under this paragraph, the right to privacy encompasses two components: (1) peace in private life and (2) private space, private activities, and private information that a natural person wants to keep from being known to others. When it comes to “peace in private life,” it refers to “the right of a natural person to exclude undue disturbance and obstruction of the peace and tranquility of his or her life by others.”³³ The purpose of this right is to prevent all kinds of harassment of private life, such as intrusion into the peace of private life of others by means of phone calls, text messages, stalking, etc. With regard to the second component, all three dimensions of privacy—space, activities, and information—must satisfy two requirements: that the natural person wants to keep them from being known to others and that they are indeed in an undisclosed state. The first requirement is about the subjective will of the right holder. The standard for this subjective will, however, is not whether a particular right holder wants to keep a matter from being known to others.

华人民共和国民法总则) [General Rules of the Civil Law of the People's Republic of China] (promulgated by the Nat'l People's Cong., Mar. 15, 2017, effective Oct. 1, 2017) (Chinalawinfo).

³¹ Article 1032 of the Civil Code stipulates that the right to privacy mainly includes private space, private activities and private information, and Article 1034 stipulates the connotation of personal information, of which the part concerning private information is subject to the provisions concerning the right to privacy. In terms of the interpretation of the normative intent of the two articles, there is a crossover relationship between personal information and privacy, and the scope of the crossover focuses on private information.

³² Civil Code, art. 1032, para. 1.

³³ WANG LIMING (王利明), RENGQUAN FA YANJIU (人格权法研究) [ON THE LAW OF PERSONALITY RIGHTS] 590 (2018).

Instead, the standard is whether a reasonable person in society would, in that circumstance, want to keep the matter from being known to others. The second requirement refers to the objective state of space, activities, and information. Private space includes not only physical space such as homes and hotel rooms but also virtual space such as e-mail and WeChat groups.³⁴ Private activities refer to “personal activities carried out by natural persons that are not related to public interests, such as daily life activities, family activities, marriage, and sexual activities.”³⁵ Private information refers to “information that is closely related to the individual and is highly private in nature, and the individual is extremely reluctant to expose to the public.”³⁶ Examples of private information include medical history information and sexual orientation information. Although private information is also personal information, it has strong personality attributes and is closely related to the protection of core personality interests. Therefore, the Civil Code includes private information in the scope of privacy and gives it stronger protection. In the WeChat Reading case, the plaintiff’s information disclosed by the defendants was the content of two books read by the plaintiff and the fact that the plaintiff read those two books. This information is not normally considered private based on the general cognitive standards of society. Therefore, the court concluded that the information at issue did not rise to the level of private information and was not protected by the right to privacy.

B. Protection of Personal Information

Prior to the enactment of the Civil Code, the General Provisions of Civil Law of 2017 specified that personal information was protected by law.³⁷ The scope of personal information, however, was left undefined. The Civil Code continued the legal protection of personal information under the previous legislation, and explicitly defined personal information within the meaning of civil law as “all kinds of information recorded electronically or by other means that can identify a specific natural person alone or in combination with other information.”³⁸ Examples of personal information include a natural person’s name, date of birth, identity document number, biometric information, address, telephone number, e-mail address, health information, and whereabouts information.

According to the Civil Code, personal information has at least three characteristics. First, personal information is identifiable. Identification includes direct identification and indirect identification. Direct identification means that

³⁴ See HUANG WEI (黄薇), *ZHONGHUA RENMIN GONGHEGUO MINFADIAN RENGEQUAN BIAN JIEDU* (中华人民共和国民法典人格权编解读) [INTERPRETATION OF THE PERSONALITY RIGHTS UNDER THE CIVIL CODE OF THE PEOPLE’S REPUBLIC OF CHINA] 196–97 (2020).

³⁵ *Id.* at 197.

³⁶ Zhang Xinbao (张新宝), *Geren Xinxi Shouji: Gaozhi Tongyi Yuanze Shiyong de Xianzhi* (个人信息收集：告知同意原则适用的限制) [*Personal Information Collection: Limits to the Application of the Principle of Informed Consent*], 6 *BIJIAOFA YANJIU* (比较法研究) [J. COMP. L.] 1, 9 (2019).

³⁷ Civil Code, art. 111.

³⁸ *Id.* art. 1034.

the information by itself is capable of identifying a specific natural person, such as the natural person's portrait or identity document number. Indirect identification means that the information needs to be combined with other information in order to achieve the effect of identifying a specific natural person. It is relatively easy to determine if a piece of information is directly identifying. But since the determination of indirectly identifying information involves analysis from technological, factual, and value perspectives, the judicial determination of such information faces many uncertainties.³⁹ That said, "there are limits on what information could be indirectly identifying—that is, there must be no undue difficulties to identify a particular individual using indirectly identifying information."⁴⁰ Indeed, most personal information is indirectly identifying. If there are no limits on indirect identification, it will lead to an overly broad scope of personal information that will hinder the reasonable use of data by enterprises.⁴¹ Second, personal information has a certain form of medium. The forms of medium specified in the statute are "electronic or other means," with "other means" referring to forms related to electronic processing. Third and finally, the holder of the rights and interests of personal information has to be a natural person. Legal persons and unincorporated organizations do not possess personal information.

Building upon its definition of personal information, the Civil Code further provides a basic legal regime for the handling of personal information to balance the conflicting interests of information protection and information usage. This legal regime requires the handling of personal information to be governed by the principles of lawfulness, justifiability, and necessity.⁴² These principles are reflected, first and foremost, in the collection of personal information. The principle of lawfulness requires that personal information be collected in accordance with the law. The principle of justifiability requires that personal information be collected for justifiable purposes and shall not be collected illegally. The principle of necessity requires the personal information legally collected to not exceed the scope necessary to achieve legitimate purposes. Violations of these principles constitute an infringement of personal information. Moreover, the Civil Code emphasizes that consent by the owner of personal

³⁹ See Cai Yibo (蔡一博), *Minfa Dian Shishi Xia Geren Xinxi de Tiaokuan Lijie yu Sifa Yingdui* (《民法典》实施下个人信息的条款理解与司法应对) [*The Interpretation of and Judicial Response to the Personal Information Provision under the Civil Code*], 5 *FALÜ SHIYONG* (法律适用) [J. L. APPLICATION] 88, 95 (2021).

⁴⁰ Han Xuzhi (韩旭至), *Geren Xinxi Gainian de Fa Jiaoyi Xue Fenxi—Yi Wangluo Anquan Fa Di 76 Tiao Di 5 Kuan Wei Zhongxin* (个人信息概念的法教义学分析——以《网络安全法》第76条第5款为中心) [*A Legal Doctrinal Analysis of the Concept of Personal Information: Centering on Article 76, Paragraph 5 of the Cyber Security Law*], 2 *J. CHONGQING UNIV.* (Social Science Edition) (重庆大学学报(社会科学版)), 161 (2018).

⁴¹ See Peng Chengxin (彭诚信) & Shi Xiaoyu (史晓宇), *Geren Xinxi Shibie Biaozhun de Yuwai Kaocha He Zai Woguo de Zhuanjin—Jiyu Meiyou Guojia Zhidu Hudong de Fenxi* (个人信息识别标准的域外考察和在我国转进——基于美欧国家制度互动的分析) [*An Extraterritorial Examination of Personal Information Identification Standards and Their Transfer in China - An Analysis Based on the Institutional Interaction of the US and European Countries*], 11 *HENAN SOCIAL SCIENCE* (河南社会科学) 8 (2020).

⁴² Civil Code, art. 1035.

information is the basis of the legal processing of personal information.⁴³ This is consistent with the “informed consent” principle adopted in the personal information protection legislation in many jurisdictions.⁴⁴ In practice, illegal collections of personal information are mainly through collecting personal information without the consent of the owner, collecting personal information with the consent of the owner but without explicitly disclosing the purposes, methods, and scope of the collection and usage, or over-collecting personal information by exceeding the disclosed purposes, methods, and scope.

The same principles also govern the use of personal information, including the provision, disclosure, processing, and transmission of personal information. Using personal information in violation of laws and regulations or agreements between the parties constitutes an infringement of personal information. In the WeChat Reading case discussed earlier, WeChat Reading failed to thoroughly disclose its usage of the information about the plaintiff’s WeChat contacts and reading activities and failed to obtain informed consent from the plaintiff. As a result, the court concluded that the defendant’s conduct infringed the plaintiff’s rights and interests of personal information.

The ultimate purpose of the bifurcated protection of personal information and privacy under the Civil Code is to promote the reasonable use of personal information and the development of the digital economy.⁴⁵ To avoid overly strict processing rules that hinder the needs of the data economy, the Civil Code provides exemptions from legal liabilities for certain personal information processing activities. These activities include reasonable processing of personal information with the consent of the owner, reasonable processing of personal information disclosed by the owner on his or her own initiative or other personal information that has already been legally disclosed (except that the owner explicitly objects to the processing of such information or that the processing of such information materially violates the owner’s interests), and other reasonable processing of personal information for the purpose of protecting the public interest or the lawful rights of the owner.⁴⁶

Apart from regulating the conduct of the processors of personal information, the Civil Code also grants certain rights to the owner of personal information, including the right to inspection, the right to reproduction, the right to correction, and the right to deletion.⁴⁷ The owner of personal information is

⁴³ *Id.*

⁴⁴ See Ji Leilei (姬蕾蕾), *Lun Tongyi Guize Zai Geren Xinxi Baohu Zhong de Shiyong—Yi Qingjing Leixing Hua Wei Shijiao* (论同意规则在个人信息保护中的适用——以情景类型化为视角) [*The Application of the Consent Principle in Personal Information Protection: From the Perspectives of Situational Types*], 2 J. SUZHOU UNIV. (SOCIAL SCIENCE EDITION) (苏州大学学报(哲学社会科学版)), 70 (2022).

⁴⁵ See Peng Chengxin (彭诚信), *Shuju Liyong de Genben Maodun Heyi Xiaochu—Jiyu Yinsi, Xinxi Yu Shuju de Fali Liqing* (数据利用的根本矛盾何以消除——基于隐私、信息与数据的法理厘清) [*How the Fundamental Contradiction of Data Use Can be Eliminated: A Jurisprudential Clarification Based on Privacy, Information and Data*], 2 TANSUO YU ZHENGMIN (探索与争鸣) [EXPLORATIONS & CONTROVERSY], 82 (2020).

⁴⁶ Civil Code, art. 1036 (Chinalawinfo).

⁴⁷ *Id.* art. 1037.

entitled to raise objections and request correction or deletion of personal information that is incorrect or has deleterious effects on the owner. The information processor is legally obligated to correct or delete such information. Failures to comply with this obligation constitutes an infringement of the rights and interests of personal information. Information processors are also subject to a number of other obligations, including the obligation not to disclose or falsify personal information, the obligation not to provide personal information unlawfully to others, as well as the obligation to ensure security and to remedy any damages to personal information.⁴⁸

C. *Distinctions Between Privacy and Personal Information*

1. Conceptual Overlaps. Before the enactment of the Civil Code, personal information was protected by the right to privacy in Chinese law, and the independent value of personal information was not recognized. This made it difficult to protect any personal information that was not private. The exact distinctions between privacy and personal information were not clear. Some scholars argued that privacy included personal information.⁴⁹ Some other scholars argued that personal information included privacy.⁵⁰ Yet other scholars argued that there was a crossover between privacy and personal information.⁵¹

The Civil Code bifurcates the legal protection of privacy and personal information. Since the promulgation of the Civil Code, courts distinguished between privacy and personal information when they adjudicated suits involving personal information. In the WeChat Reading case, for example, the court queried separately whether the information at issue was privacy and whether it was personal information. The court also determined separately whether the defendants' conduct infringed the right to privacy and whether it infringed the rights and interests of personal information. Since sometimes it is difficult to clearly distinguish privacy from personal information, the court allows the plaintiff to allege both causes of action and leave the issue for the court to settle.

The Civil Code defines the relationship between privacy and personal information in a clear manner. It divides personal information into private information and non-private information. Privacy includes private information, but

⁴⁸ *Id.* art. 1038.

⁴⁹ See Chen Hong (陈红), *Geren Xinxi Baohu de Falü Wenti Yanjiu* (个人信息保护的法律问题研究) [Legal Issues in Personal Information Protection], 3 ZHEJIANG XUEKAN (浙江学刊) [ZHEJIANG JOURNAL] 147, 148 (2008).

⁵⁰ See Hou Fuqiang (侯富强), *Woguo Geren Xinxi Baohu Lifa Moshi Yanjiu* (我国个人信息保护立法模式研究) [The Legislative Model of Personal Information Protection in China], 3 SHENZHEN DAXUE XUEBAO (RENWEN SHEHUI KEXUE BAN) (深圳大学学报(人文社会科学版)) [J. SHENZHEN UNIVERSITY (Humanities and Social Sciences Edition)] 144, 145 (2015).

⁵¹ See Zhang Xinbao (张新宝), *Cong Yinsi Dao Geren Xinxi: Liyi Zai Hengliang de Lilun yu Zhidu Anpai* (从隐私到个人信息: 利益再衡量的理论与制度安排) [From Privacy to Personal Information: Theoretical and Institutional Arrangements for Remeasuring Interests], 3 ZHONGGUO FAXUE (中国法学) [CHINA LEGAL SCIENCE] 38, 39 (2015).

not non-private information. Therefore, under the Civil Code, privacy and personal information overlap, with the overlapping part being private information. Private information also meets the three characteristics of personal information, so private information belongs to both personal information and privacy and is protected by both the right to privacy and the rights and interests of personal information.⁵² Besides private information, privacy also includes peace in personal life, private activities, and private space.

2. Similarities and Differences in the Attributes of Rights and Interests. The right to privacy and the rights and interests of personal information are both specific personality rights. The difference between the two rights is that the right to privacy is specified as a separate specific personality right,⁵³ while there are controversies on whether the rights and interests of personal information is a specific right.⁵⁴ During the drafting process of the Civil Code, the title of Chapter 6 of the Personality Rights division changed from “the Right to Privacy and the Right to Personal Information,” to “the Right to Privacy and Personal Information,” then to “the Right to Privacy and the Protection of Personal Information,” reflecting the differences in opinions among the drafters on this issue. In the end, the adoption of the normative term “the Right to Privacy and the Protection of Personal Information” in Chapter 6 of the civil Code shows that the drafters believe that personal information should be protected by law, but may not rise to the level of a specific legal right. Therefore, personal information is legally characterized as an “interest,” which includes both rights and interests. The court in the WeChat Reading case explicitly adopted the term “personal information interest.” Regardless of whether they are rights or not, privacy and personal information are both personality interests, since the core value of their protection is “personal freedom and dignity.” Treating personal information as a personality interest also reflects respect for the social existence of human beings, including their virtual identity.

The main difference between privacy and personal information protection lies in the difference in the attributes of the rights being protected. Privacy carries only personality interests, while personal information carries personality interests, property interests, and public interests in the big data era.⁵⁵ In the case of personal information, individuals often have a subjective desire to trade, wanting others to know or not caring whether others know, and objectively making their personal information available to others due to practical needs such as participation in social life. By contrast, although privacy is also a

⁵² See Civil Code, art. 1034 (Chinalawinfo).

⁵³ *Id.* art. 990.

⁵⁴ *Id.* art. 1034.

⁵⁵ See Ji Leilei (姬蕾蕾), *Qiye Shuju Baohu de Sifa Kunjing yu Poju Zhi Wei: Leixing Hua Quequan Zhi Lu* (企业数据保护的司法困境与破局之维：类型化确权之路) [Judicial Dilemmas in Enterprise Data Protection], 3 FAXUE LUNTAN (法学论坛) [LEGAL SCIENCE FORUM] 109, 113 (2022).

personality interest, individuals subjectively do not want private information to be made public, and objectively privacy cannot be freely traded and arbitrarily disposed of.⁵⁶ The Civil Code and the PIPL both adopt the model of “personal information interests” to reflect the concept of balanced interests, taking into account the similarities and differences between privacy and personal information. On one hand, this approach protects the legitimate interests of the owner of personal information and prevents damages to human dignity. On the other hand, it avoids protecting personal information in an overly absolute manner and hindering the reasonable use of personal information.

3. Differences in the Exercise of Rights and Interests. Under the Civil Code, there is a hierarchy of the protections granted to privacy and personal information, with the right to privacy being given significantly stronger protections than personal information. This hierarchy can be seen in several ways.

First, private information is both private and personal, but the provisions relating to the right to privacy take precedence, and the provisions on the protection of personal information apply only when there is no relevant provision on the right to privacy.⁵⁷

Second, there are clear differences in the conditions that need to be met for the processing of private and non-private information. Generally speaking, the processing of private information requires the consent of the owner of the information, while the processing of non-private information requires the consent of either the owner or the legal guardian. Therefore, guardians do not have the right to consent to the processing of private information on behalf of persons with limited or no legal capacity. In addition, the processing of private information requires “explicit” consent, whereas the processing of personal information requires only consent. The choice of the word “explicit” is the outcome of repeated deliberations by drafters. It means that consent to the processing of private information must be given explicitly, not by silence.⁵⁸ An information processor may process private information without the consent of the owner if a relevant law provides otherwise. However, an information processor is allowed to process personal information without the consent of the owner or legal guardian if a relevant law or administrative regulation provides otherwise. Therefore, exemptions from liability for processing private information can only be provided by laws, not by administrative regulations—a higher level of protection for private information.

⁵⁶ See Peng Chengxin (彭诚信) & Yang Siyi (杨思益), *Lun Shuju Xinxi yu Yinsi de Quanli Cengci yu Tixi Jiangou* (论数据、信息与隐私的权利层次与体系建构) [*The Hierarchy of Rights and System Construction of Data, Information and Privacy*], 2 XIBEI GONGYE DAXUE XUEBAO (西北工业大学学报) [J. NORTHWESTERN POLYTECHNIC UNIVERSITY] 79, 82 (2020).

⁵⁷ See Civil Code, art. 1034.

⁵⁸ See Wang Liming (王利明), *He Er Butong: Yinsi Quan Yu Geren Xinxi de Guize Jiefen he Shiyong* (和而不同：隐私权与个人信息的规则界分和适用) [*The Distinctions and Applications of Privacy Right and Personal Information*], 2 Legal Commentaries (法学评论) 15, 15–24 (2021).

Third, the commercial exploitation of private information is in principle not permitted. Individuals with civil capacities may license their names and likenesses to others,⁵⁹ but the Civil Code does not include privacy as a right that can be commercially exploited. There are two basic conditions for the commercial exploitation of personality elements: first, the law does not prohibit the commercial exploitation of the personality element; and second, the commercial exploitation of the personality element is not contrary to its nature. The privacy of a natural person is closely related to the dignity of the person and is related to the maintenance of the core personality interests of the person. If the commercial exploitation of privacy is allowed, it will easily lead to damage to the dignity of the natural person. Therefore, in principle, the commercial exploitation of private information is not permitted.

Compared to private information, personal information has personality interests as well as property interests. The protection of personal information should not only focus on protecting the personal interests of personal information but also take into account the objective needs of the development of the digital economy. Allowing the commercial use of personal information will not endanger the protection of the core personality interests of the information owner. As a result, the commercial use of personal information is allowed when certain conditions are met.⁶⁰

IV. THE PERSONAL INFORMATION PROTECTION LAW

A. *The Legislative Background of the PIPL*

Personal information protection is not a new legal issue, but it has become an increasingly serious problem with the development and application of data mining and analysis technologies. The most complex problem is how to reconcile the protection of personal information with its reasonable use.⁶¹ China introduced the PIPL in 2021, aiming to achieve a balance between protecting personal information and promoting its reasonable use. The legislative model of the PIPL combines legal protection of personal information with restrictions on its use. Specifically, the PIPL refines the protection norms of the Civil Code on personal information, places a high priority on the rights and interests of personal information, clarifies that the rights and interests of personal information are enjoyed by individuals, and at the same time determines the space for reasonable use of personal information by information processors. The PIPL also specifies the behavioral norms that enterprises, state agencies, and other

⁵⁹ See Civil Code, art. 993.

⁶⁰ See Peng, *supra* note 45, at 85. The commercial use of personal information is allowed when the owner's personality interests are adequately protected. In other words, the protection of personality interests is the prerequisite of the production use of data. See Peng Chengxin (彭诚信), *Lun Geren Xinxì de Shuangchong Falì Shùxing* (论个人信息的双重法律属性) [*The Dual Legal Characteristics of Personal Information*], 6 TSINGHUA LEGAL SCIENCE (清华法学) 78, 93 (2021).

⁶¹ Aimin Qi, Guosong Shao & Wentong Zheng, *Assessing China's Cybersecurity Law*, 34 COMP. L. & SECURITY REV., 1348.

information processors should follow when handling personal information and clarifies their role in the collection, storage, use, processing, transmission, and deletion of personal information. Therefore, the PIPL has shifted from an individual-oriented concept of personal information to a society-oriented one.⁶² In addition to granting many rights to information owners to maximize the protection of their rights and interests, the PIPL imposes many obligations on information processors and establishes a special administrative supervision system for personal information. This shift does not mean that the rights and interests of information owners are weakened, but rather that it is necessary to achieve a balance between the rights and interests of information owners, the property interests of information processors, and the public interests in the context of the digital age.

B. *The Relationship Between the PIPL and the Civil Code*

Article 111 and many articles of Chapter Six of the Personality Interests Division of the Civil Code involve the protection of personal information. The PIPL sets out the principles and detailed rules regarding the protection of personal information. Questions arise, therefore, as to the relationship between the two laws and how they coordinate with each other in practice.

The Civil Code Is a private law, whereas the PIPL is a mixture of private and public law, with many public-law provisions on the protection of personal information.⁶³ In this sense, the PIPL cannot be considered merely a special law of the Civil Code, since there are major differences between the two in terms of the subject matters being regulated and the purpose of regulations. There are, however, close relationships between the two laws, too. The private-law provisions that protect personal information under the PIPL are specific applications of the provisions of the Civil Code.⁶⁴ The most typical example is Article 69 of the PIPL, which provides for legal liability for violations of personal information interests. Paragraph 1 of Article 69 states: “A processor of personal information shall be liable for damages if the processing violates the personal information interests and the processor is unable to prove that it is not

⁶² Gao Fuping (高富平), *Geren Xinxi Baohu: Cong Geren Dao Shehui Kongzhi* (个人信息保护：从个人控制到社会控制) [*Personal information protection: from individual control to social control*], 3 LEGAL STUDIES (法学研究) 84, 98 (2018).

⁶³ See Peng Chengxin (彭诚信) & Xu Sumin (许素敏), *Qin Hai Geren Xinxi Quanyi Jingshen Sunhai Peichang de Zhidu Jiangou* (侵害个人信息权益精神损害赔偿的制度建构) [*Institutional Arrangements for Compensations for Mental Harms Caused by Violations of Personal Information Rights and Interests*], 3 NANJING SOCIAL SCIENCE (南京社会科学) 84, 90 (2022).

⁶⁴ See Wang Liming (王利明), *Lun Geren Xinxi Baohu Fa yu Minfa Dian de Shiqong Guanxi* (论《个人信息保护法》与《民法典》的适用关系) [*The Relationships Between the Personal Information Protection Law and the Civil Code*], 1 HUXIANG FALÜ PINGLUN (湖湘法学评论) [HUXIANG LAW REVIEW] 25, 25 (2021); Guo Feng (郭锋), Chen Longye (陈龙业) & Jia Yuhui (贾玉慧), *Geren Xinxi Baohu Fa Juti Shiyong Zhong de Ruogan Wenti Tanta—Jiyu Minfa Dian Yu Geren Xinxi Baohu Fa Guanlian de Shijiao* (《个人信息保护法》具体适用中的若干问题探讨——基于《民法典》与《个人信息保护法》关联的视角) [*Several Issues in the Application of the Personal Information Protection Law*], 1 FALÜ SHIYONG (法律适用) [LEGAL APPLICATIONS] 12, 12 (2022).

at fault.”⁶⁵ This provision establishes the principle of presumed fault, consistent with the at-fault principle established under Paragraph 1 of Article 1165 of the Civil Code. Therefore, Paragraph 1 of Article 69 of the PIPL is a special application of Paragraph 1 of Article 1165 of the Civil Code and should take precedence over the latter.⁶⁶

C. Main Provisions of the PIPL

The PIPL contains eight chapters and seventy-four articles. These provisions concern a variety of matters, including the scope of application of the law, rules on the handling of personal information, rights of the information owner, obligations of information processors, special obligations of network service providers, regulations on the handling of personal information by state organs, cross-border flow of personal information, the regulatory system for the protection of personal information, and legal liabilities.

1. Rules on Processing of Personal Information. Chapter II of the PIPL sets forth rules for handling personal information, including general rules, special provisions for handling sensitive information, and the code of conduct for state agencies as information processors. In general, this chapter sets the code of conduct from the perspective of information processors to achieve the dual purposes of protecting personal information and utilizing personal information. Several highlights of the provisions are as follows. First, the legal basis for processing personal information is expanded beyond consent, drawing upon the principles of the GDPR regime. The PIPL still uses consent as a general requirement for processing personal information, but adds several legal bases on which the processing of personal information is allowed without consent: (1) when the processing is necessary to conclude or perform a contract to which the individual is a contracting party; (2) when the processing is necessary to carry out responsibilities or duties mandated by law; (3) when the processing is necessary to deal with public health events or to protect the life, health, and property of individuals in emergency situations; (4) when the processing carried out within a reasonable scope for personal information already disclosed; (5) when the processing is carried out in news reporting for purposes of public interest; and (6) when the processing is conducted within a reasonable scope in other circumstances as provided by laws and regulations.⁶⁷ These provisions are enacted to strike a balance between the protection and utilization of personal information. Meanwhile, the PIPL adopts a differentiated

⁶⁵ Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (个人信息保护法) [Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong. Aug. 20, 2021, effective Nov. 1, 2021), art. 69 (Chinalawinfo).

⁶⁶ See Cheng Xiao (程啸), *Lun Minfa Dian yu Geren Xinxi Baohu Fa de Guanxi* (论《民法典》与《个人信息保护法》的关系) [The Relationships Between the Civil Code and the Personal Information Protection Law], 3 FALÜ KEXUE (法律科学) [Legal Science] 19, 28–29 (2022).

⁶⁷ PIPL, art. 13.

approach to consent: it provides for “separate consent”⁶⁸ and “renewed consent”⁶⁹ and stipulates that “a personal information processor shall not refuse to provide products or services on the ground that the relevant individual does not consent or withdraws consent to the processing of his or her personal information.”⁷⁰

Second, the PIPL incorporates the principle of good faith, a basic principle in civil law, as one of the basic principles to be followed in the processing of personal information.⁷¹ The principle of good faith helps to build a relationship of trust between information owners and information processors. If the trust of information owners is not protected, they will be more reluctant to share their personal information, which is detrimental to the development of the digital economy. The principle of good faith requires that processors do not handle personal information in a fraudulent, deceptive, or misleading manner, conceal the processing of personal information that a product or service performs, and obtain or process personal information through illegal channels or means. The principle of good faith is a complement to the informed consent model, which is intended to enhance self-determination for personal information. Self-determination, however, may be limited by biases in people’s rationality and risk perceptions, and in practice, the informed consent of information owners may deviate from their real intent. Therefore, the informed consent model suffers natural defects. Until a better alternative to informed consent is found, the principle of good faith is used to complement the requirement of informed consent to restore a level of trust between information owners and information processors.

Third, the PIPL pays special attention to the protection of the personal information of special owners. For minors, the PIPL defines the personal information of minors under the age of fourteen as “sensitive personal information,” which requires a special purpose and sufficient necessity for processing.⁷² The PIPL also requires that the parents or other guardians of a minor under the age of fourteen give their consent to the handling of personal information.⁷³ Meanwhile, the PIPL provides that the close relatives of the deceased have the right to review, copy, modify, or delete the “relevant” personal information of the deceased, but only for the purpose of protecting the legitimate interests of the close relatives.⁷⁴ Furthermore, these rights are subject to alternative arrangements that might be made by the deceased prior to death.⁷⁵ These provisions

⁶⁸ *Id.* art. 14 (“Separate or written consent of an individual might be required by laws or regulations for consent-based processing of personal information.”).

⁶⁹ *Id.* art. 14 (“Renewed consent shall be obtained when there are changes in the purpose, means, or categories of personal information processing.”).

⁷⁰ *Id.* art. 16.

⁷¹ *Id.* art. 5.

⁷² *Id.* art. 28.

⁷³ *Id.* art. 31.

⁷⁴ *Id.* art. 49.

⁷⁵ *Id.*

place limitations on the processing of the personal information of the deceased by close relatives, thereby protecting the privacy of the deceased and the individuals who communicated with the deceased.⁷⁶

Last but not least, the PIPL adds a provision prohibiting discrimination through the use of algorithms and big data.⁷⁷ In the era of big data, it is common for firms to make decisions through algorithms using personal information, resulting in frequent violations of the rights of personal information owners. For example, in *Hu v. Shanghai Ctrip Ltd. Co.*, the plaintiff booked a hotel room through Ctrip, a leading Chinese online travel reservation platform, for the price of RMB 2899 yuan.⁷⁸ Upon finding out that the actual price of the hotel room charged to Ctrip was only RMB 1377.63 yuan, the plaintiff sued Ctrip, alleging discrimination through big data. The court held that the plaintiff's claim had factual support, as it was reasonable for the plaintiff to suspect that he was being discriminated against by algorithms when he learned that he paid an unfairly high price, given that his personal information was in the possession of and being commercially used by the platform. The PIPL adds a provision against algorithm discrimination. The provision allows decision-making by algorithms but requires that such decision-making be transparent, fair and reasonable, and not result in unreasonable discrimination against consumers on transaction terms such as prices.⁷⁹ The PIPL also provides a remedy to consumers who are harmed by algorithm decision-making.⁸⁰ Drawing upon Article 22 of the GDPR and the American concept of *laissez-faire* governance, the PIPL does not completely prohibit algorithm decision-making to ensure necessary free space for information processing activities and to promote the development of the data market.

2. Rules on Cross-Border Transmission of Personal Information. Chapter III of the PIPL sets out the rules on the cross-border transmission of personal information. To balance the protection and utilization of personal information, the PIPL advocates cross-border rules that emphasize both protection and regulation. First, the PIPL adopts a regulatory model that ensures the security of cross-border transmission of personal information. The PIPL specifies that personal information could be transferred outside the country in the following scenarios: (a) the personal information has passed a security

⁷⁶ Cheng Xiao (程啸), *Lun Sizhe Geren Xinxi de Baohu* (论死者个人信息的保护) [*The Legal Protections of the Personal Information of the Deceased*], 5 FAXUE PINGLUN (法学评论) [Legal Commentaries] 13, 23 (2021).

⁷⁷ PIPL, art. 24.

⁷⁸ See Hu Hongfang, *Shanghai Xiecheng Shangwu Youxian Gongsi Qinquan Zeren Jiufen Ershen Minshi Panjue Shu* (胡红芳、上海携程商务有限公司侵权责任纠纷二审民事判决书) [*Hu Hongfang v. Shanghai Ctrip Commerce Co., Ltd.*], 浙江省绍兴市中级人民法院(2021)浙06民终3129号民事判决书 (Civil Judgment No. Zhe 06 Minzhong 3129).

⁷⁹ PIPL, art. 24.

⁸⁰ *Id.* (providing that individuals have rights to reject decisions made by algorithms when the decisions have significant impacts on their well beings).

assessment by the State Internet Information Office; (b) the personal information has been certified as being secure by professional institutions approved by the State Internet Information Office; (c) the transferor and transferee of the personal information sign a standardized contract approved by the State Internet Information Office; and (d) the personal information is transferred in accordance with other provisions of laws or regulations.⁸¹ At the same time, the PIPL adds a provision that strictly regulates critical information infrastructure operators and personal information processors that process a quantity of personal information reaching the threshold specified by the State Internet Information Office.⁸² Second, in order to ensure the security of personal information, the PIPL establishes a strict standard of informed consent for the transmission of personal information outside of China.⁸³ Finally, the PIPL stipulates the principle of reciprocity to safeguard national sovereignty. To prevent foreign countries from infringing on China's data sovereignty and national security, the PIPL provides that for countries or organizations outside China that endanger China's security, the State Internet Information Office may include them on a list of restricted entities to whom the transmission of personal information is restricted or prohibited.⁸⁴ Meanwhile, the PIPL provides for the principle of reciprocity in cross-border data transmission. For countries or organizations outside China that take discriminatory measures against China in terms of personal information protection, China will take reciprocal measures to safeguard its national sovereignty and security.⁸⁵

3. Personal Information Rights and Obligations. The PIPL adopts a legislative model that combines rights protection and conduct regulation. As for rights protection, the PIPL specifies that information owners have the rights to know, decide, inquire, correct, and delete, and requires personal information processors to establish a mechanism for receiving and processing requests from individuals to exercise their rights.⁸⁶ Article 45(3) of the PIPL specifically provides that "where individuals request the transfer of personal information to their designated personal information processors, if the conditions specified by the State Internet Information Office are met, personal information processors shall provide the channels for transfer."⁸⁷ Modeled after the right to data portability in the GDPR, this right is essential to data competition and protecting individuals' self-determination on data.⁸⁸ However, implementing

⁸¹ *Id.* art. 38.

⁸² *Id.* art. 40.

⁸³ *Id.* art. 39.

⁸⁴ *Id.* art. 42.

⁸⁵ *Id.* art. 43.

⁸⁶ *Id.* arts. 44–50.

⁸⁷ *Id.* art. 45(3).

⁸⁸ See Wang Qinghua (汪庆华), *Geren Xinxi Quan de Tixihua Jieshi—Jianlun Geren Xinxi Baohu Fa de Gongfa Shuxing* (个人信息权的体系化解释——兼论《个人信息保护法》的公法属性) [A Systematic

rules on the right to data portability has yet to be promulgated. The exercise of the right to data portability shall be subject to certain conditions and limitations, so as to balance the interests of information owners and information processors. As for the regulation of the behavior of information processors, the PIPL requires information processors to conduct adequate risk assessments prior to data procession⁸⁹ and to take remedial action and notify information owners in the event of data breaches or likely data breaches.⁹⁰ The PIPL also requires certain information processors to designate representatives or special agents to oversee matters related to the protection of personal information and to conduct regular compliance audits of its personal information activities.⁹¹ At the same time, a higher compliance obligation and a strict regulatory system are imposed on personal information processors that provide important Internet platform services, have a large number of users, and have complex business types.⁹²

4. Regulatory Agency for Personal Information Protection. Regarding the regulatory enforcement agency for personal information protection, there is a consistent legislative tendency in Europe and the United States to establish a unified and dedicated personal information protection regulator. The GDPR provides for regulatory enforcement by specialized national data protection agencies (DPAs), while the U.S. CCPA confers broad enforcement powers on state attorneys general in the area of personal information protection. The PIPL incorporates this model and designates the State Internet Information Office as the agency that performs the duties of personal information protection. The State Internet Information Office shall be responsible for the overall planning and coordination of personal information protection, whereas relevant departments of the State Council shall, in accordance with the PIPL and other applicable laws and administrative regulations, be responsible for personal information protection within the scope of their respective functions.⁹³ The PIPL clarifies the responsibilities of the department responsible for personal information protection,⁹⁴ specifies the measures that can be taken by the department responsible for personal information protection,⁹⁵ and stipulates

Interpretation of Personal Information Rights: The Public Law Attributes of the Personal Information Protection Law], 1 HUANQIU FALÜ PINGLUN (环球法律评论) [GLOBAL L. REV.], 69, 77 (2022).

⁸⁹ PIPL, art. 55.

⁹⁰ *Id.* art. 57.

⁹¹ *Id.* arts. 52–54.

⁹² *Id.* art. 58.

⁹³ *Id.* art. 60.

⁹⁴ *Id.* arts. 61–62.

⁹⁵ *Id.* arts. 63–64.

the filing and disposition of complaints against personal information violations.

96

5. Legal Liability. Chapter 7 of the PIPL sets out the legal liabilities for violating personal information rights. These legal liabilities include civil, administrative, and criminal liabilities. As for civil liability, Article 69 of the PIPL establishes a “presumption of fault” in ascertaining personal information violations in light of the severe information asymmetry between personal information owners and personal information processors.⁹⁷ This presumption of fault alleviates the plaintiff’s burden of proof and delivers effective remedies against personal information violations.⁹⁸ In the WeChat Reading case, for example, the evidence the plaintiff was able to submit to the court was limited to information accessible to him and did not include information about Tencent’s algorithms and other internal technical data that would demonstrate infringement of rights. The court, therefore, applied the presumption of fault and shifted the burden of proof to Tencent. Moreover, the PIPL provides for a public-interest litigation mechanism to ensure adequate remedies in cases involving massive data breaches and large numbers of victims.⁹⁹ As for administrative liability, the PIPL provides for compelled compliance, confiscation of illegal income, fines, suspension of business, revocation of relevant business permits, and revocation of business licenses.¹⁰⁰ As for criminal liability, the PIPL stipulates that if the acts of personal information processors or the staff of government agencies performing personal information protection duties constitute crimes, criminal liability shall be pursued in accordance with the law.¹⁰¹ In sum, the PIPL builds a comprehensive network of legal liabilities for personal information violations, linking together civil, administrative, and criminal remedies.

V. REMAINING ISSUES

A. *The Dichotomy of Privacy and Personal Information Protection*

Chapter VI of the Civil Code on Personal Rights not only defines personal information but also distinguishes private information from non-private information, protecting them differently in accordance with their categorization. Private information is protected by both the right to privacy and the rights and interests of personal information. The handling of another person’s private

⁹⁶ *Id.* art. 65.

⁹⁷ *Id.* art. 69.

⁹⁸ Jiang Bixin (江必新) & Guo Feng (郭峰), *Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa Tiaowen Lijie yu Shiyong* (《中华人民共和国个人信息保护法》条文理解与适用) [*Interpretations and Applications of the Personal Information Protection Law*] 605 (2021).

⁹⁹ PIPL, art. 70. “Public-interest litigation” under China’s Civil Procedure Law is akin to class-action lawsuits in the United States.

¹⁰⁰ *Id.* arts. 66–68.

¹⁰¹ *Id.* art. 71.

information requires either the “express consent” of the person who has the right to privacy or has to be done in accordance with the law. Therefore, under the Civil Code, the fundamental requirement for the processing of personal information is the protection of privacy. Article 1032 of the Civil Code, which prohibits any organizations or individuals from infringing citizens’ right to privacy,¹⁰² is binding on Chinese courts. Chinese courts have to ascertain whether the personal information at issue is “private” and is therefore entitled to privacy protection. In the *WeChat Reading* case, the court held that the owner of non-private information suffers personality and property damages only when the non-private information is excessively processed. Because of this limitation, judicial remedies may not be available if non-private information is not excessively processed.

Unlike the Civil Code, which adopts the concept of “private information,” the PIPL adopts the concept of “sensitive information.”¹⁰³ The PIPL distinguishes between sensitive information and non-sensitive information in order to better protect the fundamental rights of natural persons such as human dignity and personal freedom, as well as their legal rights such as property rights. Sensitive information includes information on biometric identification, religious beliefs, specific identity, health care, financial accounts, personal whereabouts, etc.¹⁰⁴ A question arises, therefore, as to the relationship between private information and sensitive information. The two types of information may overlap—that is, some information is both private and sensitive, such as sexual orientation. Some information, such as information about personal hobbies, is private but not sensitive. Some other information, such as information about race, ethnicity, religious beliefs, political opinions, and facial features, is sensitive but not private. Under this dichotomy of privacy and personal information protection, the relationship between private information and sensitive information has become an unavoidable issue, which poses great challenges for Chinese courts in their handling of personal information protection.

In practice, even for the same type of personal information, differences in information processing practices may lead to the conclusion that the right to privacy is violated in some cases, but not in others. For example, in *Liu v. Le Element Company*, an app developed by the defendant collected the plaintiff’s location information.¹⁰⁵ The court held that the information collected was for the purpose of identifying the plaintiff and did not disrupt his peace of life. Therefore, the court held that the defendant’s action did not constitute an infringement of the plaintiff’s right to privacy.¹⁰⁶ In *Lin Mou v. Zhang Mou*,

¹⁰² Civil Code, art. 1032.

¹⁰³ PIPL, arts. 28–32.

¹⁰⁴ *Id.* art. 28.

¹⁰⁵ See *Liu Ruibo yu Le Yuansu Keji* (Beijing) Gufen Youxian Gongsi Yinsi Quan Jiufen Ershen Panjue Shu (刘瑞博与乐元素科技(北京)股份有限公司隐私权纠纷二审民事判决书) [*Liu Ruibo v. Happy Elements Technology (Beijing) Co., Ltd.*, (2020)京01民终8911号 (Beijing First Interim. People’s Ct. 2020)].

¹⁰⁶ *Id.*

however, the defendant made public the plaintiff's court hearing time and place by posting a microblog on the website.¹⁰⁷ The court held that such behavior would easily cause the plaintiff to be outed by internet searches and threaten the peace of his private life, thus constituting an infringement of privacy.¹⁰⁸ It is foreseeable that Chinese courts and judges will face a growing number of such scenario-specific challenges. They will need to constantly make comprehensive judgments based on multiple factors, such as the act of processing information, the type of information, and the possible impact of the information processing, before they can effectively distinguish between privacy and personal information and provide appropriate remedies.

B. The Interface of Personal Information Processing Rules with Multiple Processing Scenarios

In theory, the consent rule is undoubtedly the best legal structure to guarantee the information owner's control over his or her information considering its normative power and impact. In practice, however, this may not turn out to be the case, especially with the advent of the big data era. The collection and use of personal information have reached an unprecedented level, and the function of the consent rule has gradually failed. In response to the need to develop the data economy, the PIPL expands the legal bases for personal information processing to seven, which include "personal consent" and "necessity for processing contracts."¹⁰⁹ However, there are overlaps and contradictions in the application of these two legal bases.

The PIPL provides strict rules on consent,¹¹⁰ while granting the right to withdraw consent for information.¹¹¹ It also requires separate consent in specific circumstances.¹¹² An exception to consent is provided for when the processing of personal information is required for the "provision of products or services."¹¹³ Taking these provisions together, if a processor of personal information uses "contractual necessity," that is, processing personal information is

¹⁰⁷ See Zhang Jinwu Lin Ligu Wangluo Qinquan Zeren Jiufen Eshen Panjue Shu (张金武、林礼国网络侵权责任纠纷二审民事判决书) [Zhang Jinwu v. Lin Ligu], (2020)鲁14民终1348号 (Dezhou Interim People's Ct. 2020).

¹⁰⁸ *Id.*

¹⁰⁹ Article 13 of the PIPL stipulates that a processor of personal information may handle personal information only in one of the following circumstances: (a) to obtain the consent of the individual; (b) necessary for the conclusion or performance of a contract to which the individual is a party; (c) necessary for the performance of legal duties or legal obligations; (d) in response to a public health emergency, or in an emergency to protect the life, health and property of natural persons (e) necessary for the implementation of news reporting, public opinion supervision and other acts in the public interest within a reasonable range of personal information; (f) other circumstances provided for by laws and administrative regulations. See PIPL, art. 13.

¹¹⁰ PIPL, art. 14.

¹¹¹ *Id.* art. 15.

¹¹² *Id.* arts. 14, 23, 25, 26, 29, 39.

¹¹³ Article 16 provides that a processor of personal information shall not refuse to provide products or services on the grounds that the individual does not consent to the processing of his or her personal information or withdraws his or her consent to the processing of personal information, unless the processing of personal information is necessary for the provision of the product or service. *Id.* art. 16.

necessary for performing contracts in the provision of goods or services, as the legal basis of processing personal information, the questions that arise are three-fold. First, what criteria govern the determination of “contractual necessity”? The hidden nature of data technology and the diverse arrays of data use make it difficult for information owners to know the extent of “contractual necessity,” and this will become a gap in information protection that deserves further study. Second, if the legal basis of “contractual necessity” is adopted, it will become an exception to the consent rule. Under these circumstances, individuals cannot withdraw their consent, and the collection of personal information becomes a contractual obligation to perform. As a result, the information processor may be able to bypass the consent requirement. In this way, the consent rule has the possibility of becoming obsolete. Finally, how to define “products or services”? For example, Alipay provides payment services, health services, life services, and so on, which form a service ecological chain. It would be rather challenging to define “contractual necessity” for this wide array of services. How to apply the legal standards to these diversified scenarios still needs further studies and refinements.

C. Different Obligations for Different Information Processors

The PIPL imposes special obligations to protect personal information on large personal information processors commensurate with their control and influence, thereby strengthening the regulation of large personal information processors. However, the PIPL does not provide for the obligations of small personal information processors. Rather, it adopts an evasive attitude by stipulating that the State Internet Information Office shall coordinate with relevant government agencies to formulate special personal information protection rules and standards for small personal information processors. The differential treatment for large and small information processors is questionable in two ways.

First, the PIPL provides that the obligations of small information processors require special rules and standards to be set by the State Internet Information Office at a later date. It is unclear, however, whether the PIPL already exempts small information processors from some of the obligations specified therein. If so, there is also a great amount of controversy as to whether such exemptions are reasonable. There is currently a worldwide consensus that large personal information processors with a certain degree of control and influence should be subject to enhanced regulation, but there is no consensus as to whether small personal information processors should be exempted from regulation. If small information processors are subject to special rules and standards on the protection of personal information, how should the general rules on the obligations of personal information processors under the PIPL be applied? Although the PIPL has made it clear that special rules and standards for the protection of personal information shall be established in accordance with the PIPL, if exemptions are permitted, there will inevitably be a conflict between the rules and standards

for small personal information processors and the general rules. Resolving the potential conflicts between the special and general rules may prove challenging.

Second, the PIPL only sets relatively minimal rules on the obligations required of large information processors. Article 58 of the PIPL draws upon the concept of “gatekeepers” introduced by a draft of the EU Digital Marketplace Act published in December 2020. The EU Digital Marketplace Act, however, is primarily an antitrust law that coordinates the competing interests of platforms (“gatekeepers”) and third-party merchants, for example by stipulating that “gatekeepers” should not compete unequally with third-party merchants and should allow third-party merchants to complete transactions through their own apps or websites outside of their platforms. China, however, has introduced “gatekeeper” provisions in personal information protection, imposing on “gatekeepers” that provide important internet platform services the obligation to ensure that the providers of products or services on the platforms are required to handle personal information lawfully and to protect the rights and interests of personal information owners. It also allows the gatekeeper to impose penalties on product or service providers who seriously violate the norms of the platforms to stop providing services. These provisions amount to a change in the regulatory purpose of the original “gatekeeper” rule, and therefore the regulatory content of the PIPL, which imposes a series of additional obligations on large personal information processors, needs to be further refined.

D. “Separate Consent” and “Security Assessment” for Cross-Border Data Flows

The protection of personal information has been a global issue primarily because of the cross-border flows of personal information.¹¹⁴ The protection of personal information across borders should not only pay attention to the impact of cross-border flows of personal information on national security but also should protect the rights and interests of personal information owners. It needs to not only protect data sovereignty in cross-border flows but also balance the relationship with data freedom. Therefore, cross-border data flows concern a variety of interests, including national interests, industrial interests, and consumer interests. Too stringent regulations are not conducive to data uses and the development of the digital economy, whereas too lenient regulations may bring national security risks. Therefore, the PIPL takes a cautious approach to the cross-border flows of personal information and reenacts the data localization policy in the Cybersecurity Law. This policy, while beneficial to the protection of China’s data sovereignty, creates obstacles to cross-border data flows.

¹¹⁴ Shao Guosong (邵国松) & Huang Qi (黄琪), *Geren Shuju Baohu Quanjie Ronghe de Qushi yu Tiaozhan* (个人数据保护全球融合的趋势与挑战) [Trends and Challenges in the Global Convergence of Personal Data Protection], 4 SHANGHAI JIAOTONG DAXUE XUEBAO (上海交通大学学报) [JOURNAL OF SHANGHAI JIAO TONG UNIVERSITY], 158 (2021).

While the PIPL has enhanced China's regulations on cross-border data flows, several issues still remain. First, global rules on cross-border data flows are premised on the consensus that the consent of the information owner is a prerequisite for the transmission of personal information across national borders. But nations differ as to the details. China requires stricter "separate consent" than general consent for the cross-border transmission of personal information. When a processor needs to transmit personal information abroad, it must separately specify the details of the information processing and obtain explicit authorizations from the individual whose information is being processed. While this stricter requirement might be beneficial for consumers, it leads to inconsistencies in global rules on personal data and may unduly hinder cross-border data flows.

Second, the PIPL specifies that the transmission of personal information across the border by critical information infrastructure and personal information processors that handle personal information up to a certain amount requires a security assessment. The factors to be taken into account in the security assessment need to be further clarified. In addition, it needs to be further clarified whether those who are not subject to security assessments can voluntarily apply for them.

Finally, there is also a lot of controversy over the interface between China's cross-border rules and those of other countries. For example, the GDPR requires other countries or regions to meet the EU's standards for personal data protection in order to be included in the "adequate protection" white list, while China's PIPL requires the foreign recipients of personal information to meet the personal information protection standards stipulated in that law. In other words, the term "equivalent level of protection" has a different meaning in China.

E. Administrative Penalties and Discretions

Article 66 of the PIPL stipulates the amount of fine that personal information processors are liable for when they violate their personal information handling obligations. It distinguishes between cases subject to a fine of up to one million yuan and cases subject to a fine of up to fifty million yuan or five percent of the previous year's turnover, depending on the severity of the violations.¹¹⁵ But there are no provisions on minimum fines. In other words, there

¹¹⁵ PIPL, art. 66. By contrast, the GDPR distinguishes between cases where the fine is capped at the higher of €10 million or 2% of global revenue and cases where the fine is capped at the higher of €20 million or 4% of global revenue. The CCPA distinguishes between general violations, willful violations and violations of children's rights, with different fines depending on, inter alia, the subjective state of mind. It provides for a civil fine of up to \$2,500 per violation in general, and up to \$7,500 per violation in special circumstances, such as when the violation is willful or involves a business, service provider, contractor or other people with actual knowledge of personal information of a minor under the age of 16. The civil fine is not to exceed \$7,500 per violation in general and \$7,500 per violation in special circumstances, such as when the violation is intentional or involves a business, service provider, contractor, or another person having actual knowledge of personal information of a minor under the age of 16.

is a possibility of too low a fine, which might significantly reduce the deterrent effect of the law. Therefore, it is necessary to further clarify the enforcement standards and refine the applications of the corresponding rules in practice. Meanwhile, in addition to the two categories of administrative fines specified in the PIPL, the law needs to clarify if there are other factors to be considered in determining the amount of administrative penalties for personal information violations, and how to determine whether the circumstances are serious enough to warrant a higher penalty. These rules need to be spelled out more clearly to limit administrative discretion.

F. Limited Practical Impact

The relatively stable and sluggish legal regulatory model cannot respond quickly and effectively to the new compliance needs of enterprises in the marketing of their business services and products, which are characterized by the changing nature of enterprises' personal information handling activities due to the increasing pace of technological advances. This suggests that, at a macro level, there are limitations on the effectiveness of the legal regulatory model in guiding companies' activities in handling personal information. Therefore, the enactment of the PIPL is not the end of privacy and personal information protection in China. Nor does it necessarily guarantee that the realistic needs for personal information protection will be met, that personal information leakage will be reduced and that harms will be minimized. Based on past empirical studies, the enactment of the Cybersecurity Law has not led to a significant increase in the intensity of personal information protection in website operations, and the compliance level of most website operators is still low, with many obvious data security loopholes.¹¹⁶ Compared to the Cybersecurity Law, the PIPL provides more comprehensive and detailed rules for the personal information handling activities, as well as corresponding provisions for the rights and obligations of individuals and information handlers. But the inherent limitations of the legal regulatory model still persist. For example, what are the minimum standards for deletion or de-identification technologies? Are there different risk levels for such technologies? And what is the scope of the personal information protection for the deceased? These are all issues that the PIPL fails to adequately address.

VI. CONCLUSIONS

China's vast privacy and personal information protection regime rests on three pillars: the Constitution, which lays the foundation for privacy and

¹¹⁶ Shao Guosong (邵国松) et al., *Woguo Wangzhan Geren Xinxi Baohu Shuiping Yanjiu—Jiyu Wangluo Anquan Fa dui Woguo 500 Jia Wangzhan de Shizheng Fenxi* (我国网站个人信息保护水平研究——基于《网络安全法》对我国 500 家网站的实证分析) [Research on the level of personal information protection of websites in China - an empirical analysis of 500 websites in China based on the Cybersecurity Law], 3 XINWEN JIZHE (新闻记者) [JOURNALISTS], 55, 55–65 (2018).

personal information protection, and the Civil Code and the PIPL, which implement the Constitution's protection of individual freedom and dignity. With their own focuses and reasonable divisions of labor, the Civil Code and the PIPL work together to achieve the coordination of privacy and personal information rights and interests protection and the rational use of personal information. A central purpose of the Civil Code is to distinguish privacy from personal information from the perspective of civil rights protection, and on this basis, personal information is divided into private information and non-private information, with a higher degree of protection being given to the right to privacy. The PIPL is the first special law on personal information protection in China. Drawing upon international experience, the PIPL regulates the handling of personal information with "informed consent" at its core. The interpretation of the PIPL and its relation to the application of the Civil Code is an important task for the protection of privacy and personal information in China.

China's legal regime for privacy and personal information protection faces a number of issues that require further consideration and optimizations. First, despite the legislative distinction between privacy and personal information, in judicial practice, judges still need to grapple with the question of whether the personal information involved in a lawsuit is private or only general personal information. Second, the law provides for seven legal bases for handling personal information, with a view to promoting the sustainable and healthy development of the data economy. But it still needs to further refine how the legal standards apply in different processing scenarios. Third, the law distinguishes large and small information processors in terms of processing obligations. The regulation of large processors has been strengthened and their data security obligations have been increased, while small processors are exempted from certain obligations. Fourth, China has enacted stricter requirements for cross-border flows of personal data but still lacks effective measures to deal with the problems and obstacles that may be encountered in implementing the requirements. Fifth, for those who are subject to administrative penalties for personal information violations, the law sets an upper limit for the fine without setting a lower limit, and the power of administrative discretion is rather large. Therefore, there is a possibility of an unreasonably low fine. Finally, many provisions of the Civil Code and the PIPL are still unclear. Even though it has a guiding effect on the compliance of enterprises in handling personal information, the practical impact of the laws on information processors might be limited. With all these issues, China still has a long way to go to have a well-functioning legal regime for privacy and personal information protection.