Law and Practice of Personal Data Protection in the Digital World: A Comparison Between China, the EU, and the U.S.

Charles Chao Wang*

This Article makes an in-depth comparative and empirical study on China's personal data protection legal system and its public enforcement at the state and local levels. The 2016 Cybersecurity Law and the 2021 Personal Information Protection Law (PIPL) regulate important personal data protection issues such as public interests' protection and very large online platforms' (VLOPs) gatekeeper mechanism. China's regulatory focus has shifted from network infrastructure construction to cybersecurity and personal data protection. Unlike the U.S. and the EU, China has delegated law enforcement to the Cyberspace Administration of China (CAC) and the Ministry of Industry and Information Technology (MIIT) under a unique twin peaks model at the state level. The CAC and local agencies focus on regulating data processors based on catch-all provisions, while the MIIT focuses on regulating app developers' activities, such as the collection and use of personal data. At the local level, China decentralized regulatory powers to local governmental agencies. In the public enforcement of data protection laws, the EU, the U.S. and China have divergent institutional structures and administrative penalties. These divergences are caused by China's political and economic context, especially the national strategy to facilitate the development of VLOPs for global competition. China's public interests are embodied in the ideological censorship and national security review of users' information by data processors. It is concerning that the Chinese government might enlarge their control over the dissemination of information. China should learn from the EU's experience in tackling specific problems of automated decision-making. To supervise the gatekeepers, Chinese law needs to strike a balance between encouraging the development of VLOPs and protecting personal data.

[*] © 2025 Charles Chao Wang, Assistant Professor, Durham Law School, Durham University, Durham, UK. Email: charleswang5999@outlook.com. This research is supported by the Hong Kong Research Grants Council's General Research Fund project "China's Data Protection Regime in the Context of Fintech." (RGC Ref No. 14601524). I sincerely appreciate the valuable comments on an earlier draft of this paper provided by Robin Hui Huang, Lei Chen, Zehra Gulay Kavame Eroglu, Lingling Hou, and Yang Chen, as well as the feedback from participants at the 2024 Annual Meeting of the American Society of Comparative Law held at Texas A&M University School of Law. I am also grateful to the editors for their meticulous work and to Yiman Li for her outstanding research assistance. Any remaining errors are my own.

I. INTRODUCTION

Personal data protection in the digital world has become more and more important.[1] In 2018, the Facebook user data leakage incident attracted worldwide attention and criticism.[2] Big tech companies and other data processors have gained a gatekeeper power, which stems from the fact that they serve as infrastructure for digital markets.[3] Advances in artificial intelligence algorithms allow data processors to monitor all kinds of useful information twenty-four seven without interruption.[4] For example, robo-advisors help financial investors grasp investment

[1] In this Article, "personal data" and "personal information" are used interchangeably. For more discussions on the relationships between corelated concepts of privacy and data protection, *see* Yang Li and Min Yan, *The Conceptual Barrier to Comparative Study and International Harmonisation of Data Protection Law*, 51 HONG KONG L.J. 917 (2021); Yang Li and Min Yan, *Distinguishing Data Protection from Privacy: A Transnational Perspective,* SSRN, https://ssrn.com/abstract=4753123 (last visited Aug. 1, 2024).

[2] Lily Hay Newman, *What Really Caused Facebook's 500M-User Data Leak*, WIRED, (Apr. 6, 2021), https://www.wired.com/story/facebook-data-leak-500-million-users-phone-numbers/ (last visited Aug. 1, 2024).

[3] Sabeel K. Rahman, *Private Power, Public Values: Regulating Social Infrastructure in a Changing Economy*, 39 CARDOZO. L. REV. 5 (2017); Lina M. Khan, *Sources of Tech Platform Power*, 2 GEO. L. TECH. REV. 325 (2018).

[4] Merriam-Webster, *Artificial Intelligence*, at https://www.merriam-webster.com/dictionary/artificial%20intelligence (last visited Nov. 1, 2024).

information in real time and make rational investment decisions.[5] Artificial intelligence technology provides data processors with stronger tools for surveillance.[6] Digital platforms can, with the help of algorithms, obtain information about the list of websites visited by employees, supervise employees' work progress, and infringe on employees' privacy.[7] Data processors excessively collect personal information, which seriously infringes upon the data subject's right of control over personal information.[8] These latest technological developments exacerbate the improper use of personal data by data processors, which may adversely impact individuals' freedom of expression[9] and create social risks such as employment discrimination.[10]

In recent years, many jurisdictions around the world have introduced comprehensive personal data protection laws to cope with the challenges brought by the era of big data. The European Union (EU) and the United States (U.S.) have refined their personal data protection standards, and further improved the regulation of data processors. In 2016, the EU formulated the General Data Protection Regulation (GDPR), which stipulates the obligations of data processors and the rights of data subjects in detail.[11] In 2022, the EU issued the Digital Services Act (DSA)[12] and

[5] Robin Hui Huang, Charles Chao Wang, and Olivia Xin Zhang, *The Development and Regulation of Robo-Advisors in Hong Kong: Empirical and Comparative Perspectives*, 22(1) J. OF CORP. L. STUD. 229 (2022).

[6] Saby Ghoshray, *Employer Surveillance Versus Employee Privacy: The New Reality of Social Media and Workplace Privacy*, 40 N. KY. L. REV. 593 (2013).

[7] Antonio Aloisi & Elena Gramano, *Artificial Intelligence Is Watching You at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context*, 41 COMP. LAB. L. & POL'Y J. 95 (2019).

[8] Sandra Wacther, *Data Protection in the Age of Big Data*, 2 NATURE ELECTRONICS 6 (2019). For example, Uber uses algorithms to monitor employees' clock-in times and work performance, ranking them according to a five-star standard. *See* Leonie Cater and Melissa Heikkila, *Your Boss is Watching: How AI-Powered Surveillance Rules the Workplace, Companies Are Buying Increasingly Intrusive Artificial Intelligence Tools to Keep an Eye on Their Workers*, POLITICO, (May 27, 2021), https://www.politico.eu/article/ai-workplace-surveillance-facial-recognition-software-gdpr-privacy/ (last visited Aug. 1, 2024).

[9] Pauline T. Kim, *Electronic Privacy and Employee Speech*, 87 CHI.-KENT L. REV. 901 (2012).

[10] Claudia Schubert& Marc-Thorsten Hutt, Economy-on-Demand and the Fairness of Algorithms, 10 EUR. LAB. L.J. 3 (2019); Pauline T. Kim, *Genetic Discrimination, Genetic Privacy: Rethinking Employee Protections for a Brave New Workplace*, 96 NW. U. L. REV. 1497 (2002).

[11] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, 2016 O.J. (L 119) 1.

[12] *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC*

the Digital Markets Act (DMA),[13] which regulate online gatekeeper platforms to set out new standards for dealing with societal risks on freedom of expression and other fundamental rights. In the U.S., there has been no GDPR-style comprehensive legislation at the federal level, and each state has its own data protection rules.[14] The California Consumer Privacy Act (CCPA) is most typical, making California a trailblazer in the U.S.[15] The regulatory models of the EU and the U.S. have had a profound impact on the personal data protection legislation of other jurisdictions in the world, including China.[16] For example, many multinational companies have adopted the practice of applying GDPR standards on a global scale, exemplifying the "Brussels effect."[17]

To facilitate competition with developed jurisdictions, China's National People's Congress (NPC) passed the Cybersecurity Law in 2016[18] and the Personal Information Protection Law (PIPL) in 2021.[19] Together with existing statutes, they streamlined China's gatekeeper mechanism of data processors and balanced the protection of personal data and public interests. There are several important reforms, such as requiring certain data processors to have a "personal information protection officer" (Geren Xinxi Baohu Fuzeren, or 个人信息保护负责人 in Chinese) and stipulating additional obligations for very large online

(Digital Services Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065 (last visited Aug. 1, 2024).

[13] *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 Sept. 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828* (Digital Markets Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925 (last visited Aug. 1, 2024).

[14] Pauline T. Kim, *Privacy Rights, Public Policy, and the Employment Relationship*, 57 OHIO ST. L.J. 671 (1996).

[15] Mariana Renke, *TikTok and Instagram Know What You Did Last Summer—And the Federal Government Will Not Be the One to Put a Stop to It*, 2023 U. ILL. J.L. TECH. & POL'Y 451 (2023).

[16] In this Article, "China" refers to mainland China, or the People's Republic of China.

[17] Antonio Aloisi and Elena Gramano, *Artificial Intelligence Is Watching You at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context*, 41 COMP. LAB. L. & POL'Y J. 95 (2019); Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2012); Anupam Chander, *When the Digital Services Act Goes Global*, 38 BERKELEY TECH. L.J. 1067 (2023); Dawn Carla Nunziato, *The Digital Services Act and the Brussels Effect on Platform Content Moderation*, 24 CHI. J. INT'L L. 115, 117 (2023).

[18] Zhonghua Renmin Gongheguo Wangluo Anquan Fa (中华人民共和国网络安全) [Cybersecurity Law of the PRC] (promulgated by the National People's Congress, Nov. 7, 2016, effective June 1, 2017) [hereinafter Cybersecurity Law].

[19] Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Personal Information Protection Law of the PRC] (promulgated by the National People's Congress, Aug. 20, 2021, effective Nov. 1, 2021) [hereinafter PIPL].

platforms (VLOP).[20] In order to adapt to the era of artificial intelligence, China has stipulated obligations for data processors to deal with new challenges like automated decision-making. To enforce these rules effectively, China has delegated regulatory authority to governmental agencies, among which the Cyberspace Administration of China (CAC, Guojia Hulianwang Xinxi Bangongshi, or 国家互联网信息办公室) and the Ministry of Industry and Information Technology (MIIT, Gongye He Xinxihua Bu, or 工业和信息化部) play a pivotal role.[21] The CAC and the MIIT undertake different regulatory powers and supplement each other functionally, so this Article calls it a "twin peaks model." To date, the most typical and famous case is the case of DiDi, which received the most severe punishment by the CAC. As China's Uber-like ride-sharing app, DiDi was established in 2012, with its main business including ride-hailing services and the operation of mobile apps.[22] In 2022, a fine of 8.026 billion yuan was imposed on DiDi, and a fine of 1 million yuan was imposed on Cheng Wei, chairman and CEO of Didi, and Liu Qing, president of Didi, respectively.[23]

This Article makes an in-depth study of China's personal data protection system and its public enforcement from doctrinal, comparative, and empirical perspectives.[24] Part II discusses the historical development of China's personal data protection laws. It includes three stages: network infrastructure construction, improvement of cybersecurity, and enhanced

[20] Wendy Ng, *The Role of Competition Law in Regulating Data in China's Digital Economy*, 84 A.B.A. L.J. 841 (2022).

[21] *China's CAC and MIIT Undertake Parallel Consultations on Draft Measures for Cyber Incident Reporting*, (Jan. 24, 2024), https://www.hoganlovells.com/en/publications/chinas-cac-and-miit-undertake-parallel-consultations-on-draft-measures-for-cyber-incident-reporting#:~:text=The%20CAC%20is%20China's%20cyber,the%20technology%20and%20telecommunications%20industries, HOGAN LOVELLS (last visited Aug. 1, 2024).

[22] Prospectus of American Depositary Shares of DiDi, (June 10, 2021), https://www.sec.gov/Archives/edgar/data/1764757/000104746921001194/a2243272zf-1.htm, SEC (last visited Aug. 1, 2024).

[23] OFFICIAL WEBSITE OF THE CAC, *The Decision of the CAC to Impose Administrative Penalties Related to Cybersecurity Review on DiDi Global Co., Ltd. According to Law* (July 21, 2022), https://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm (last visited Aug. 1, 2024).

[24] For more discussions on public and private enforcement of Chinese law, *see* Robin Hui Huang, *Rethinking the Relationship Between Public Regulation and Private Litigation: Evidence from Securities Class Action in China*, 19(1) THEORETICAL INQUIRIES IN L. 333 (2018); Shaowei Lin, *Private Enforcement of Chinese Company Law: Shareholder Litigation and Judicial Discretion*, 4 CHINA LEGAL SCI. 73 (2016); Guanghua Yu, *Derivative Actions in China: Path Dependence Revisited*, 11 J. OF COMP. L. 151 (2016); Jun Wang, *On Cases Against Corporate Managers for Breaching Their Duty of Loyalty and/or Duty of Diligence in China*, 10 FRONTIERS L. CHINA 77 (2015).

protection of personal data. Part III analyzes the current legal framework of China's personal data protection legal system, including the regulatory framework, major rights of data subjects, and major obligations of data processors. Part IV conducts an empirical study on the public enforcement of China's personal data protection laws by the CAC and the MIIT under the twin peaks model. Part V compares and analyzes the regulatory models of China, the EU, and the U.S. (California), focusing on their convergences and divergences. It summarizes the advantages and disadvantages of the Chinese model in terms of public interest protection (such as the review of sensitive data, ideological censoring, national security review, and automation decision-making) and the gatekeeper mechanism. Based on these analyses, this Article puts forward relevant reform suggestions. Part VI is the conclusion.

II. HISTORICAL DEVELOPMENT OF PERSONAL DATA PROTECTION LAWS IN CHINA

A. Stage 1 (2000-2016): Network Infrastructure Construction

This stage was characterized by the State Council and the MIIT's efforts to construct China's internet infrastructure after China joined the WTO. In 2000, the State Council, which is China's central government, formulated the Telecommunications Regulation.[25] It applies to telecommunications activities or telecommunications-related activities in China.[26] Telecommunications business operators, including data processors, shall operate in accordance with the law, abide by business ethics, and accept governmental supervision and inspection.[27] The competent authorities are the information industry authorities under the State Council, which refers to the later established MIIT and its provincial branches.[28] The MIIT, established in March 2008, is the State Council's department in charge of industry and information industry.[29] The Information and Communication Administration under the MIIT is

[25] Zhonghua Renmin Gongheguo Dianxin Tiaoli (中华人民共和国电信条例) [Telecommunications Regulation of the PRC] (promulgated by the State Council, Sept. 25, 2000, effective Sept. 25, 2000, amended in 2014 and 2016) [hereinafter Telecommunications Regulation].

[26] *Id.*

[27] Article 4 of the 2016 Telecommunications Regulation.

[28] Article 3 of the 2016 Telecommunications Regulation.

[29] *State Council of the People's Republic of China, The State Council's Decision on Implementing the Comprehensive Reform of the Administrative System*, State Council (Aug. 23, 2014), https://english.www.gov.cn/state_council/2014/08/23/content_281474983035940.htm.

responsible for the management of the internet industry.[30] At this stage, China enforced data protection laws based on the single regulator model (the MIIT).

In 2000, the State Council formulated the Regulation on Internet Information Service.[31] Internet information service refers to the service activities that provide information to internet users.[32] The MIIT and its provincial branches shall supervise and manage internet information services according to law.[33] The relevant governmental agencies responsible for supervising press, publication, education, health, drug, industry and commerce, public security, and national security shall supervise and administer internet information content within their respective scope of authorities.[34]

In 2012, the NPC formulated the NPC Decision.[35] It proposed that the state protect electronic information that can identify individual citizens and involve citizens' personal privacy.[36] In addition, it stipulates basic principles for the protection of personal electronic information.[37] On June 28, 2013, the MIIT issued the Personal Information Provisions.[38] The MIIT and its provincial branches shall supervise and manage the protection of personal information of telecommunications and internet users.[39] Telecom business operators and internet information service providers are the main objects of regulation, which need to be responsible for personal information security.[40] Internet information service providers shall stop collecting and using users' personal information and provide

[30] *Id.*

[31] Hulianwang Xinxi Fuwu Guanli Banfa (互联网信息服务管理办法) [Regulation on Internet Information Service] (promulgated by the State Council, Sept. 25, 2000, effective Sept. 25, 2000, amended in 2011).

[32] Article 2 of the 2000 Regulation on Internet Information Service.

[33] Article 18 of the 2000 Regulation on Internet Information Service.

[34] Article 18 of the 2000 Regulation on Internet Information Service.

[35] Guanyu Jiaqiang Wangluo Xinxi Baohu De Jueding (关于加强网络信息保护的决定) [Decision on Strengthening Network Information Protection] (promulgated by the National People's Congress, Dec. 28, 2012, effective Dec. 28, 2012) [hereinafter NPC Decision].

[36] *Id.*

[37] Article 2 of the 2012 NPC Decision.

[38] Dianxin He Hulianwang Yonghu Geren Xinxi Baohu Guiding (电信和互联网用户个人信息保护规定) [Provisions on Protecting the Personal Information of Telecommunications and Internet Users] (promulgated by the MIIT, July 16, 2013, effective Sept. 1, 2013) [hereinafter Personal Information Provisions].

[39] Article 3 of the 2013 Personal Information Provisions.

[40] Article 6 of the 2013 Personal Information Provisions.

users with services for cancelling their numbers or accounts after users terminate their use of telecommunications services.[41]

B. Stage 2 (2016-2021): Improvement of Cybersecurity

1. The 2016 Cybersecurity Law

This phase has several characteristics. First, the personal information protection legislation gradually developed, emphasizing the maintenance of cybersecurity. Second, at the central government or state level, there was a shift in institutional dynamics. A new twin peaks model was formed under the 2016 Cybersecurity Law.[42] The MIIT is no longer the single most important regulator, and started to share regulatory powers with the CAC, the Ministry of Public Security (MPS, Gongan Bu, or 公安部), and the State Administration for Market Regulation (SAMR, Guojia Shichang Jiandu Guanli Zongju, or 国家市场监督管理总局). On May 4, 2011, the CAC was established to undertake the network information security coordination responsibilities previously undertaken by the MIIT.[43] The CAC is responsible for the overall planning and coordination of cybersecurity work and related supervision and management.[44] Third, at the local government level, China decentralized regulatory powers to local governmental agencies. Relevant governmental departments above the county level have started to assume the responsibilities of cybersecurity management.[45] Last but not least, public enforcement is reinforced. There are two levels of administrative punishment, including the network operator (data processor) and the person in charge who is directly responsible.[46]

In 2019, the CAC, the MIIT, the MPS and the SAMR jointly issued the Methods for Identifying Illegal and Irregular Collection and Use of

[41] Article 9 of the 2013 Personal Information Provisions.

[42] *See Translation of the Cybersecurity Law of the People's Republic of China* (effective June 1, 2017), DIGICHINA, STAN. UNIV. (last visited Dec. 11, 2024), https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

[43] State Council of the People's Republic of China, *The State Council's Decision on Implementing the Comprehensive Reform of the Administrative System*, State Council (Aug. 23, 2014), https://english.www.gov.cn/state_council/2014/08/23/content_281474983035940.htm.

[44] *Id.*

[45] Article 8 of the 2016 Cybersecurity Law. Some scholars view the scattered supervisory responsibility as a weakness of the current Chinese data protection regime. *See* Yang Li and Min Yan, *The Conceptual Barrier to Comparative Study and International Harmonisation of Data Protection Law*, 51 HONG KONG L.J. 917 (2021).

[46] Article 64 of the 2016 Cybersecurity Law.

Personal Information by Apps.[47] The law sets practicable rules in many technical details.[48]

First, the phrase "apps that illegally collect and use personal information" is defined. For example, it covers situations where the rules for collecting and using personal information are not disclosed, and the purpose, method and scope of collecting and using personal information are not clearly stated.[49]

Second, the phrase "apps that do not express the purpose, method, and scope of collecting and using personal information" is defined. For example, it covers situations where the purpose, method, and scope of collecting and using personal information by an app are not listed one by one.[50]

Third, the phrase "apps that collect and use personal information without users' consent" is defined. For example, it covers situations where an app collects personal information before obtaining users' consent or opening the permission to collect personal information.[51]

Fourth, the phrase "apps that fail to provide functions to delete or correct personal information as required by law" is defined. For example, it covers situations where an app fails to provide effective functions for correcting, deleting personal information and cancelling user accounts.[52]

Fifth, the phrase "apps that provide personal information to others without consent" is defined. For example, it covers situations where an app accesses a third-party application and provides personal information to the third-party application without the user's consent.[53]

Sixth, the phrase "apps that fail to provide the function of deleting or correcting personal information as required by law" is defined. For example, it covers situations where an app fails to provide effective functions for correcting, deleting personal information, and cancelling user accounts.[54]

[47] App Weifa Weigui Shouji Shiyong Geren Xinxi Xingwei Rending Fangfa Zhengqiu Yijian Gao (App违法违规收集使用个人信息行为认定方法征求意见稿) [Draft of Methods for Identifying Illegal and Irregular Collection and Use of Personal Information by Apps] (promulgated by the CAC, the MIIT, the MPS and the SAMR, May 5, 2019) [hereinafter App Identifying Methods Draft].

[48] *Id.*

[49] Article 1 of the 2019 App Identifying Methods Draft.

[50] Article 2 of the 2019 App Identifying Methods Draft.

[51] Article 3 of the 2019 App Identifying Methods Draft.

[52] Article 6 of the 2019 App Identifying Methods Draft.

[53] Article 5 of the 2019 App Identifying Methods Draft.

[54] Article 6 of the 2019 App Identifying Methods Draft.

2. The 2021 Data Security Law

In 2020, China enacted the Civil Code.[55] Article 111 stipulates the right to personal information. Article 1034 stipulates that private information in personal information shall be subject to the provisions on privacy rights. The law prohibits the illegal collection, use, processing, transmission, illegal sale, provision, or disclosure of personal information. Based on the principles and spirits of the Civil Code, China enacted a Data Security Law in 2021.[56] Under the 2021 Data Security Law, "data" (Shuju, or 数据) refers to any record of information by electronic or other means.[57] Data security requires taking necessary measures to ensure that data is effectively protected and lawfully used in a continuous manner.[58] The CAC is responsible for coordinating network data security as well as other governmental agencies that regulate public security, state security, industry, telecommunications, transportation, finance, natural resources, health, education, science, and technology are responsible for data security supervision within their respective areas of responsibility.[59]

The state aims at protecting the data rights of individuals and organizations. It encourages the rational and effective use of data, ensures the orderly and free flow of data, and promotes the development of the digital economy.[60] To achieve this agenda, the state establishes a unified, efficient, and authoritative mechanism for data security risk assessment, reporting, information sharing, monitoring, and early warning.[61]

[55] Zhonghua Renmin Gongheguo Minfadian (中华人民共和国民法典) [Civil Code of the PRC] (promulgated by the National People's Congress, May 28, 2020, effective Jan. 1, 2021).

[56] Zhonghua Renmin Gongheguo Shuju Anquan Fa (中华人民共和国数据安全法) [Data Security Law of the PRC] (promulgated by the National People's Congress, June 10, 2021, effective Sept. 1, 2021) [hereinafter Data Security Law].

[57] Translation of the Cybersecurity Law of the People's Republic of China (effective June 1, 2017), DIGICHINA, STAN. UNIV. (last visited Dec. 11, 2024), https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

[58] Article 3 of the 2021 Data Security Law.

[59] Article 6 of the 2021 Data Security Law.

[60] Article 7 of the 2021 Data Security Law.

[61] Article 22 of the 2021 Data Security Law.

C. *Stage 3 (From 2021): Enhanced Protection of Personal Data*

1. The 2021 PIPL

The 2021 PIPL is groundbreaking in many aspects, such as the applicable scope.[62] The law not only applies to domestic activities dealing with the personal information of natural persons, but also stipulates for the first time the extraterritorial jurisdiction.[63] The law applies to activities outside China that process the personal information of natural persons within China, for the purpose of (1) providing products or services to natural persons within China; (2) analyzing and evaluating the behavior of natural persons within China; and (3) in other circumstances.[64] A data processor outside China shall set up a special organization or designate a representative within China to handle matters related to personal information protection and submit their contact information to the regulatory authority.[65] "Personal information" refers to all kinds of information relating to identified or identifiable natural persons recorded electronically or by other means, excluding information after anonymization.[66] Personal information processing activities include collection, storage, use, processing, transmission, provision, disclosure, deletion, etc.[67] The main regulatory objects under the 2021 PIPL are personal information processors, namely organizations and individuals who independently decide the purpose and method of processing in personal information processing activities.[68] The data processor has the obligation to ensure the security of personal information.[69]

It is noteworthy that the law stipulates additional obligations for VLOPs which provide important internet platform services with a large

[62] The PIPL not only stipulates the general framework for personal data protection, but also helps to address some of the issues in specific areas. For more discussion on personal data protection in online contracting, smart contract, and other issues, *see* Jia Wang & Lei Chen, *Will Innovative Technology Result in Innovative Legal Frameworks? Smart Contracts in China*, 26(6) EUR. REV. OF PRIV. L. 921 (2018); Qin Zhou, *Whose Data Is It Anyway? An Empirical Analysis of Online Contracting for Personal Information in China*, 31(1) ASIA PACIFIC L. REV. 73 (2022).

[63] For more discussion on extraterritorial jurisdiction of China's Securities Law, *see* Robin Hui Huang, Charles Chao Wang, Yuqi Zhou, Sunny Xiyuan Li, *Extraterritorial Jurisdiction of China's New Securities Law: Policies, Problems and Proposals*, 22(2) J. OF CORP. L. STUD. 1 (2022).

[64] Article 3 of the 2021 PIPL.

[65] Article 53 of the 2021 PIPL.

[66] Article 4 of the 2021 PIPL.

[67] *Id.*

[68] Article 73 of the 2021 PIPL.

[69] Article 9 of the 2021 PIPL.

number of users and complex business types. Large digital platforms are typical VLOPs, which are the most typical subject of personal information protection. Digital platforms are profit-making enterprises that have quasi-legislative, quasi-executive, and quasi-judicial power in the process of platform content governance.[70] VLOPs should establish a personal information protection compliance system, as well as an independent organization composed mainly of external members to supervise the protection of personal information. They should follow the principles of openness, fairness, and impartiality; formulate platform rules; and clarify the norms of personal information processing and the obligations of personal information protection of product or service providers within the platform. When product or service providers on the platform handle personal information in serious violation of laws, VLOPs should stop providing services to them. VLOPs should publish social responsibility reports on personal information protection on a regular basis.[71]

In order to better protect personal data, scholars suggested the establishment of auditing system for artificial intelligence data transparency.[72] In August 2023, the CAC released the Draft on the Compliance Audits Measures.[73] It reviews and evaluates whether the personal information processing activities of a data processor comply with the law.[74] Data processors that handle the personal information of more than one million people shall conduct compliance audits at least once a year, and other data processors shall conduct compliance audits at least once every two years.[75] Data processors may conduct compliance audits on their own,[76] and regulators may also require data processors to conduct compliance audits.[77] The audit organization can request

[70] Hannah Bloch-Wehba, *Global Platform Governance: Private Power in the Shadow of the State*, 72 SMU L. REV. 27 (2019).

[71] Article 58 of the 2021 PIPL.

[72] Shlomit Yanisky-Ravid & Sean K. Hallisey, *Equality and Privacy by Design: A New Model of Artificial Intelligence Data Transparency via Auditing, Certification, and Safe Harbor Regimes*, 46 FORDHAM URB. L.J. 428 (2019); Pauline T. Kim, *Auditing Algorithms for Discrimination*, 166 U. PA. L. REV. ONLINE 189 (2017).

[73] Geren Xinxi Baohu Hegui Shenji Guanli Banfa Zhengqiu Yijian Gao (个人信息保护合规审计管理办法征求意见稿) [Draft of Measures for the Administration of Personal Information Protection Compliance Audits] (promulgated by the CAC, Aug. 3, 2023) [hereinafter Compliance Audits Measures Draft].

[74] Article 3 of the 2023 Compliance Audits Measures Draft.

[75] Article 4 of the 2023 Compliance Audits Measures Draft.

[76] Article 5 of the 2023 Compliance Audits Measures Draft.

[77] Article 6 of the 2023 Compliance Audits Measures Draft.

assistance when they access relevant documents or materials.[78] In principle, the compliance audit shall be completed within ninety working days.[79]

2. Basic Principles

First, data processors shall abide by the principles of legality, legitimacy, necessity, and good faith. The data processor shall not process personal information through misleading, fraud, coercion, or other means,[80] and shall not endanger national security, social and public interests, or the legitimate rights of others.[81] It has the obligation to manage users' information.[82] The processing of personal information shall have a clear and reasonable purpose, shall be directly related to the purpose of processing, shall adopt a method that has the least impact on the rights of individuals, and shall not collect excessive personal information.[83] Unless otherwise provided for by law, the retention period of personal information shall be the minimum period necessary to complete processing.[84]

Second, data processors shall abide by the principle of openness, transparency, and informed consent.[85] The rules for processing personal information shall be disclosed, and the purpose, method, and scope of the processing shall be clearly stated.[86] Under normal circumstances, individuals have the right to know and decide on the processing of their personal information and the right to restrict or refuse the processing of their personal information by others.[87] The data processor needs the individual's separate consent to process and disclose the personal information it processes.[88]

[78] Article 8 of the 2023 Compliance Audits Measures Draft.
[79] Article 9 of the 2023 Compliance Audits Measures Draft.
[80] Article 5 of the 2021 PIPL.
[81] Article 6 of the 2016 Telecommunications Regulation.
[82] Article 5 of the 2012 NPC Decision.
[83] Article 6 of the 2021 PIPL.
[84] Article 19 of the 2021 PIPL.
[85] Article 22 of the 2016 Cybersecurity Law.
[86] Article 7 of the 2021 PIPL.
[87] Article 44 of the 2021 PIPL.
[88] Article 25 of the 2021 PIPL.

III. THE CURRENT LEGAL FRAMEWORK FOR PERSONAL DATA PROTECTION IN CHINA

A. *Regulatory Framework*

1. Twin Peaks Model

As mentioned, China has gradually established and streamlined a twin peaks model dominated by the CAC and the MIIT. The CAC's major powers include:

> (1) formulating specific rules and standards for personal information protection;
>
> (2) formulating special rules and standards for personal information protection for "small personal information processors" (Xiaoxing Geren Xinxi Chulizhe, or 小型个人信息处理者), for processing sensitive personal information (Mingan Geren Xinxi, or 敏感个人信息), and for new technologies and applications such as face recognition and artificial intelligence;
>
> (3) supporting the research, development, promotion, and application of secure and convenient electronic identity authentication technology and promoting the construction of public services for online identity authentication;
>
> (4) promoting the construction of a social service system for personal information protection and supporting relevant institutions to carry out personal information protection assessment and authentication services;
>
> (5) improving the complaint and reporting mechanism.[89]

In March 2018, the National Computer Network and Information Security Management Center under the MIIT was adjusted to be managed by the CAC.[90]

At the state level, regulators other than the CAC and the MIIT chiefly include the MPS and the SAMR.[91] For example, the 2016

[89] Article 62 of the 2021 PIPL.

[90] *China's Cyberspace Authorities Set to Gain Clout in Reorganization*, DigiChina, STAN. UNIV. (last visited Dec. 11, 2024), https://digichina.stanford.edu/work/chinas-cyberspace-authorities-set-to-gain-clout-in-reorganization/.

[91] Cyber Administration of China (CAC). Cyber Administration of China (last visited Dec. 11, 2024), https://www.cac.gov.cn/; Ministry of Industry and Information Technology (MIIT) Ministry of Industry and Information Technology (last visited Dec. 11, 2024), https://www.miit.gov.cn/. Ministry of Public Security (MPS) Ministry of Public Security (last visited

Telecommunications Regulation stipulates that no subject shall steal or destroy other people's information,[92] otherwise the public security organizations and state security organizations will impose administrative penalties.[93] In 2019, the MPS and other agencies formulated the Guide to Internet Personal Information Security Protection.[94] It is worth noting that the National Data Administration (NBS, Guojia Shuju Ju, or 国家数据局) was established on October 25, 2023 to undertake the supervision and management of big data, which is managed by the National Development and Reform Commission (NDRC, Guojia Fazhan He Gaige Weiyuanhui, or 国家发展和改革委员会).[95] Due to its short history, it remains to be seen what impact the NBS will exert on the current twin peaks model.

The 2021 PIPL stipulates the division of regulatory powers between the central and local governments. At the local level, the relevant departments of local governments above the county level are responsible for supervision within their jurisdiction.[96] They mainly include local public security departments and local market supervision administration.[97] The main responsibilities of the regulators in personal information protection include: (1) publicity and education of personal information protection, guidance, and supervision of data processors; (2) accepting and dealing with complaints and reports; (3) evaluating the protection of personal information such as applications and publishing the results; (4) investigating and dealing with illegal activities; and (5) other duties.[98] There are regulatory measures that the regulator can take, including: (1) inquiries and investigations; (2) consulting and copying relevant materials; (3) carrying out on-site inspection; (4) inspecting, sealing, or detaining relevant equipment and articles; (5) interviewing the

Dec. 11, 2024), https://www.mps.gov.cn/; State Administration for Market Regulation (SAMR) State Administration for Market Regulation (last visited Dec. 11, 2024), https://www.samr.gov.cn/.

[92] Article 58 of the 2016 Telecommunications Regulation.

[93] Article 67 of the 2016 Telecommunications Regulation.

[94] Hulianwang Geren Xinxi Anquan Baohu Zhinan (互联网个人信息安全保护指南) [Guide to Internet Personal Information Security Protection] (promulgated by the MPS, Apr. 10, 2019, effective Apr. 10, 2019).

[95] Translation of Establishing the National Data Administration (Mar. 2023), DigiChina, STAN. UNIV. (last visited Dec. 11, 2024), https://digichina.stanford.edu/work/translation-establishing-the-national-data-administration-march-2023/.

[96] *Personal Information Protection Law of the People's Republic of China*, adopted by the Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021, (China).

[97] Article 60 of the 2021 PIPL.

[98] Article 61 of the 2021 PIPL.

principal person in charge of the data processor; and (6) requiring data processors to conduct a compliance audit.[99]

2. Legal Liability

If the data processor illegally processes personal information, there are several punishment measures that the regulators can take, including ordering corrections be made (Zeling Gaizheng, or 责令改正); issuing a warning (Jinggao, or 警告); confiscating illegal gain (Moshou Weifa Suode, or 没收违法所得); imposing a fine (Fakuan, or 罚款); ordering the suspension or termination of app services (Zeling Zanting, or 责令暂停或者终止app服务); revoking a license or cancelling filing (Diaoxiao Xukezheng Huozhe Quxiao Beian, or 吊销许可证或者取消备案); closing a processor's website (Guanbi Wangzhan, or 关闭网站); and prohibiting relevant responsible personnel from engaging in network service business (Jinzhi Youguan Zeren Renyuan Congshi Wangluo Fuwu Yewu, or 禁止有关责任人员从事网络服务业务).[100]

Under the 2016 Cybersecurity Law, if a data processor infringes on the right to personal information, the regulator may impose a fine of one to ten times the illegal gain.[101] If there is no illegal gain, a fine of less than 1 million yuan will be imposed, and a fine of 10,000 to 100,000 yuan will be imposed on the person in charge who is most directly responsible and other persons directly responsible.[102] Under the 2021 PIPL, if the data processor refuses to make corrections, it shall also be fined up to one million yuan.[103] A fine of 10,000 to 100,000 yuan shall be imposed on the person in charge directly responsible and other persons directly responsible.[104] If the circumstances are serious, regulators at or above the provincial level may order to make corrections, confiscation of illegal gains and impose a fine of no more than fifty million yuan or no more than five percent of the turnover of the previous year.[105] Regulators may order the suspension of relevant business activities or the suspension of business for rectification, or notify the relevant competent authorities to

[99] Articles 63, 64 of the 2021 PIPL.

[100] Article 11 of the 2012 NPC Decision; Article 66 of the 2021 PIPL.

[101] *Cybersecurity Law of the People's Republic of China* (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017) (China).

[102] Article 64 of the 2016 Cybersecurity Law.

[103] *Personal Information Protection Law of the People's Republic of China*, adopted by the Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021, (China).

[104] Article 67 of the 2021 PIPL.

[105] Article 66 of the 2021 PIPL.

revoke relevant business licenses. Moreover, regulators can impose a fine of 100,000 to one million yuan on the person in charge directly responsible and other persons directly responsible, which may be prohibited from serving as the management of the relevant enterprise and the personal information protection officer for a certain period of time.[106] In addition, illegal acts will be recorded in credit files and made public.[107] Those who violate the administration of public security will be punished according to the law.[108]

B. *The Major Rights of Data Subjects*

1. The Right to Know and Consent

Before processing personal information, the data processor shall truthfully, accurately, and completely inform the data subject of the name and contact information of the data processor in a conspicuous manner and in clear and understandable language.[109] An individual shall have the right to request the data processor explain the personal information processing rules.[110] Where a data processor processes sensitive personal information, it shall also inform the individual of the necessity of processing sensitive personal information and the impact on the individual's rights.[111] There are exceptions to the right to know, including when: (1) confidentiality is stipulated by law; (2) the failure to inform individuals in a timely manner could protect the life, health, or property safety of natural persons in emergency situations;[112] and (3) such notification will hinder state organizations from performing statutory duties in processing personal information.[113]

The general premise of personal data processing is to obtain the consent of the data subject.[114] Where a data processor processes the personal information of a minor under the age of fourteen, it shall obtain the consent of the minor's parents or other guardians.[115] Without the consent of the person to be collected, the data processor shall not provide

[106] *Id.*
[107] Article 67 of the 2021 PIPL.
[108] Article 71 of the 2021 PIPL.
[109] Article 17 of the 2021 PIPL.
[110] Article 48 of the 2021 PIPL.
[111] Article 30 of the 2021 PIPL.
[112] Article 18 of the 2021 PIPL.
[113] Article 35 of the 2021 PIPL.
[114] Article 41 of the 2016 Cybersecurity Law.
[115] Article 31 of the 2021 PIPL.

personal information to others unless the specific individual cannot be identified after processing and the information cannot be restored.[116] There are exceptions to the right of consent, including: (1) circumstances that are necessary for the conclusion and performance of a contract to which the individual is a party and (2) circumstances that are necessary for the implementation of human resources management in accordance with legally formulated labor rules and collective contracts.[117]

If the processing of personal information is based on an individual's consent, such consent shall be made voluntarily and explicitly by the individual on the premise of being fully informed.[118] In specific situations, individual consent or written consent shall be obtained for the processing of personal information.[119] If for the purpose of personal information processing the method of processing and the type of personal information to be processed are changed, personal consent must be obtained again.[120] The individual has the right to withdraw his/her consent.[121] The data processor shall provide a convenient way to withdraw consent and shall not refuse to provide products or services on this basis.[122]

When image collection and personal identification equipment are installed in public places, the personal images and identification information collected can only be used for the purpose of maintaining public security, unless the individual has separately agreed to it.[123] The data processor can process legally disclosed personal information within a reasonable scope unless expressly rejected by the individual.[124] If the data processor processes the personal information that has been disclosed and has a major impact on the rights of the individual, it shall obtain the consent of the individual.[125]

2. The Right to Copy and Right of Portability

With certain exceptions, an individual has the right to access and copy his/her personal information, and the data processor shall provide it in a timely manner. The statutory exemptions mainly refer to

[116] Article 42 of the 2016 Cybersecurity Law.
[117] Article 13 of the 2021 PIPL.
[118] Article 14 of the 2021 PIPL.
[119] Article 13 of the 2021 PIPL.
[120] Article 14 of the 2021 PIPL.
[121] Article 16 of the 2021 PIPL.
[122] Articles 15, 16 of the 2021 PIPL.
[123] Article 26 of the 2021 PIPL.
[124] Article 13 of the 201 PIPL.
[125] Article 27 of the 2021 PIPL.

circumstances when: (1) information should be kept confidential or does not need to be disclosed according to the law[126] and (2) such notification will hinder state organizations from performing their statutory duties.[127] If an individual requests the transfer of personal information to another data processor designated by the individual and meets the conditions specified by the CAC, the data processor shall provide the means of transfer.[128] This is similar to the right to data portability under the GDPR.[129]

3. The Right to Rectification and Erasure

Personal information processing shall avoid adverse effects on personal rights caused by the inaccuracy and incompleteness of personal information.[130] If an individual discovers that his/her personal information is inaccurate or incomplete, he/she shall have the right to request the data processor rectify it.[131] This right is functionally similar to the right to rectification under the GDPR.[132]

The data processor should actively delete personal information when the purpose of processing has been achieved, cannot be achieved, or is no longer necessary to achieve. If the storage period prescribed by statutes has not expired, or the deletion of personal information is technically difficult to achieve, the data processor shall stop all processing activities other than storage and necessary security protection.[133] This right is functionally similar to the GDPR's right to erasure or right to be forgotten.[134]

4. The Right of Litigation

If the data processor refuses an individual's request to exercise its rights, it shall give reasons, and the individual may file a lawsuit.[135] Where a data processor infringes upon the civil rights of data subjects, it shall bear civil liabilities.[136] Where two or more data processors jointly process

[126] Article 18 of the 2021 PIPL.

[127] Article 35 of the 2021 PIPL.

[128] Article 45 of the 2021 PIPL.

[129] Article 20 of the 2016 GDPR.

[130] Article 8 of the 2021 PIPL.

[131] Article 43 of the 2016 Cybersecurity Law; Article 46 of the 2021 PIPL.

[132] Article 16 of the 2016 GDPR.

[133] Article 8 of the 2012 NPC Decision; Article 43 of the 2016 Cybersecurity Law; Article 47 of the 2021 PIPL.

[134] Article 17 of the 2016 GDPR.

[135] Article 50 of the 2021 PIPL.

[136] Article 11 of the 2012 NPC Decision.

personal information and cause damage, they shall bear joint civil liability.[137] The data processor's civil liability shall be "presumed fault liability" (Guocuo Tuiding Zeren, or 过错推定责任).[138] The liability for damages shall be determined according to the loss suffered by the individual or the gains obtained by the data processor.[139] If it is difficult to determine, the amount of compensation shall be determined by courts according to the precise situation.[140]

In addition to the individuals who have received the infringement, the procuratorate, statutory consumer organizations and the CAC designated organizations can also file lawsuits against the infringement of many individual rights.[141] This arrangement combines the advantages of public enforcement and private litigation.[142]

C. Major Obligations of Data Processors

Data processors are regulated in different laws with different definitions. For example, the 2021 PIPL regulates "data processors,"[143] while the 2016 Cybersecurity Law regulates network operators.[144] This Article uses the official term of "data processor" under the 2021 PIPL.

1. General Obligations

The data processor shall not illegally collect, use, process, or transmit other people's personal information. It is forbidden to illegally trade, provide, or disclose other people's personal information, or engage in personal information processing activities that endanger national security and public interests.[145] A data processor shall keep the user

[137] Article 20 of the 2021 PIPL.

[138] Article 69 of the 2021 PIPL.

[139] Article 68 of the 2021 PIPL.

[140] Article 69 of the 2021 PIPL.

[141] Article 70 of the 2021 PIPL.

[142] Due to the underdevelopment of private litigations, the Chinese government has designed public and quasi-public enforcement mechanisms to facilitate the enforcement of laws in China. This can be found in various legal areas, such as securities law and environmental law. *See* Flora Huang, *In Defence of China's Public Enforcement in Equity Market*, 21.10 INT'L CO. AND COM. L. REV. 327 (2010); Chunyan Ding & Huina Xiao, *A Paper Tiger? Prosecutorial Regulators in China's Civil Environmental Public Interest Litigations*, 32(3) FORDHAM ENV'T L. REV. 323 (2021); Juan Chu, *From Peripheral Actors to Established Players: Environmental NGOs' Participation Through Public Notice-And-Comment Procedures and Environmental Public Interest Litigation in China*, 33(149) J. OF CONTEMP. CHINA 790 (2023).

[143] Article 73 of the 2021 PIPL.

[144] Article 40 of the 2016 Cybersecurity Law.

[145] Article 10 of the 2021 PIPL.

information it collects strictly confidential and establish and improve the user information protection system.[146] It shall take measures to ensure that personal information processing activities are legal, including formulating internal management systems and operating procedures, implementing classified management of personal information, and adopting security technical measures.[147] A data processor shall not steal or obtain personal information by other illegal means and shall not illegally sell or provide personal information to others.[148]

2. Formulate and Publish Rules for Information Collection and Use

The data processor shall formulate rules for the collection and use of users' personal information and publish them on its websites.[149] Otherwise, the MIIT shall order it to make corrections within a time limit, give a warning, and impose a fine of less than 10,000 yuan.[150] If the situation is serious, the MIIT can impose a fine of 10,000 to 30,000 yuan, which will be announced to the public.[151]

Article 2 of the 2019 App Identifying Methods Draft enumerates situations where apps fail to publish the rules of information collection and use, including: (1) having no privacy policy in the app, or having no rules for collecting and using personal information in the privacy policy; (2) failing to prompt users to read the privacy policy and other collection rules in obvious ways, such as a pop-up window when the app runs for the first time; (3) having privacy policy and other collection rules that are difficult to access;[152] and (4) having collection and use rules, such as a privacy policy, that are difficult to read.[153]

3. Compliance Audit

The data processor shall conduct regular compliance audits on its compliance with laws and administrative regulations in processing

[146] Article 40 of the 2016 Cybersecurity Law.

[147] Article 51 of the 2021 PIPL.

[148] Articles 1, 3 of the 2012 NPC Decision; Article 44 of the 2016 Cybersecurity Law.

[149] Article 41 of the 2016 Cybersecurity Law.

[150] Article 22 of the 2013 Personal Information Provisions.

[151] Article 23 of the 2013 Personal Information Provisions.

[152] For example, if after entering the main interface of the app it takes more than four clicks to access the privacy policy or collection rules.

[153] For example, the text may be too small and dense, the color of the text too light or ambiguous, or the simplified Chinese version is not provided.

personal information.[154] Under any of the following circumstances, the data processor shall conduct an assessment of the impact of personal information protection in advance and record the processing situation: (1) when processing sensitive personal information; (2) when using personal information to make automated decisions; (3) when entrusting the processing of personal information, providing personal information to other data processors, and disclosing personal information; (4) when providing personal information overseas; or (5) during other personal information processing activities that have a significant impact on individual rights.[155]

The impact assessment shall include the following information: (1) whether the purpose and method of personal information processing are legal, reasonable, and necessary; (2) the impact on personal rights and security risks; and (3) whether the protective measures taken are legal, effective, and appropriate to the degree of risk. The impact assessment reports and processing records shall be kept for at least three years.[156]

4. Take Relief Measures

In case of any personal information infringement, the data processor shall immediately take remedial measures and notify regulators and individuals.[157] The contents of the notice shall include personal information leakage, tampering, types of information lost, reasons, and possible harm.[158] The data processor shall establish a user complaint processing mechanism and reply to the complainant within fifteen days.[159] It shall handle the complaint in a timely manner according to the law.[160]

IV. EMPIRICAL ANALYSIS OF PUBLIC ENFORCEMENT OF PERSONAL DATA PROTECTION LAWS IN CHINA

A. *Enforcement by the CAC and Local Agencies*

1. Distribution of Cases by Time

This Article analyzes administrative penalty cases of online personal information infringement under the 2021 PIPL and the 2016

[154] Article 54 of the 2021 PIPL.

[155] Article 55 of the 2021 PIPL.

[156] Article 56 of the 2021 PIPL.

[157] Article 4 of the 2012 NPC Decision; Article 42 of the 2016 Cybersecurity Law.

[158] Article 57 of the 2021 PIPL.

[159] Article 12 of the 2013 Personal Information Provisions.

[160] Article 65 of the 2021 PIPL.

Cybersecurity Law.[161] As Table 1 shows, from August 20, 2021 (when the 2021 PIPL took effect) to December 31, 2023, there were fifty-one cases in total enforced by the CAC and local governmental agencies.

Table 1: Distribution of Cases by Time

Year	Number of Cases	Percentage
2022	40	78.4%
2023	11	21.6%
Total	51	100%

Table 1 shows the distribution of cases of administrative penalties for online personal information infringement by time. Most cases took place in 2022, accounting for 78.4% of all cases. A typical case is the case of Caifuhui Technology (Shenzhen) Co. in 2022.[162] The large number of cases in 2022 shows that the enactment of the 2021 PIPL has had a significant influence on online personal data protection, which is exemplified in a peak in law enforcement cases. The number of cases in 2023 showed a decline.

2. Hierarchical Distribution of Regulators

Table 2: Hierarchical Distribution of Regulators

Hierarchical Level	Number of Cases	Percentage
State (the CAC)	2	3.9%
Municipal (Public Security Bureau)	12	23.5%
District/County (Public Security Bureau)	37	72.6%
Total	51	100%

Table 2 shows the hierarchy of regulators that have imposed administrative penalties on data processors. The regulatory agencies are mainly at the district/county level, and there are few cases at the state level (two cases).

[161] This author searched the official websites of the CAC and the MIIT, as well as authoritative databases such as Beida Fabao, with keywords such as "personal information protection law" and "cybersecurity law."

[162] Decision of the Futian Branch of Shenzhen Public Security Bureau on Administrative Penalty for Caifuhui Keji Shenzhen Youxian Gongsi (财阜荟科技深圳有限公司) [Caifuhui Technology Shenzhen Co., Ltd.] (2022) No. 36509.

This shows that the CAC's administrative penalties focused on companies with great social impact, including DiDi and CNKI.[163] At the local level, the CAC mainly relies on municipal and district/county-level local governments for law enforcement (forty-nine cases) and draws on the power of local public security bureaus. This shows that China decentralized regulatory powers to local governmental agencies (municipal and district/county levels) to enforce data protection laws more efficiently, which will be discussed in Part V of the article.

3. Geographical Distribution of Regulators

Table 3: Geographical Distribution of Regulators

Geographical Distribution of Regulators	Number of Cases	Percentage
The Central Government (the CAC)	2	3.9%
Jiangsu Province	*21*	*41.2%*
1. Suqian City	7	13.7%
2. Xuzhou City	4	7.8%
3. Taizhou City	3	5.9%
4. The other six cities in Jiangsu Province (no more than two cases)	7	13.7%
Guangdong Province	*28*	*54.9%*
Shenzhen City	28	54.9%
Total	51	100%

Table 3 shows that the local enforcement cases were highly concentrated in two provinces (Jiangsu and Guangdong). In Guangdong, all of the cases took place in Shenzhen, which is the biggest city in the province and one of China's biggest cities. In Jiangsu, cases were spread across several cities within the province. There may be a number of explanations for this. First, administrative penalty cases are not as publicized as court cases. It is highly possible that many other provinces chose not to publicize cases. Second, Jiangsu and Guangdong provinces have the most developed economies and most advanced digital platform

[163] Official website of the CAC, *The Decision of the CAC to Impose Administrative Penalties Related to Cybersecurity Review on DiDi Global Co., Ltd. According to Law* (July 21, 2022), https://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm (last visited Aug. 1, 2024); official website of the CAC, *The Decision of the CAC to Impose Administrative Penalties Related to Cybersecurity Review on CNKI According to Law*, (Sept. 6, 2023), https://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm (last visited Aug. 1, 2024).

industries.[164] Third, as an economic center of Guangdong Province and China's Silicon Valley, Shenzhen has fostered the growth of many big tech companies such as Huawei and Tencent.[165] The distribution of high-tech industries in Jiangsu Province is relatively scattered.[166]

4. Data Processors by Identity and Category

Table 4: Data Processor Identity

Identity of Data Processors	Number of Cases	Percentage
Organization	50	98%
Natural Person	1	2%
Total	51	100%

Table 4 shows that the punished data processors are mainly organizations, with only one natural person data processor. In this case, Fan Moumou allowed members of his/her website to publish false statements and information and collect membership fees by using the identity information he/she obtained from others.[167] Natural persons affiliated with data processor organizations can be punished too, such as DiDi Global's Chairman Cheng Wei and President Liu Qing.[168] They were fined one million yuan each.[169] This shows that enterprises and other organization data processors are the main actors in the infringement of online personal information because they usually have more economic and social resources.

[164] *China's Top Manufacturing Regions*, CAMA Ltd. (Sept. 26, 2024), https://camaltd.com/china-top-manufacturing-regions/, last visited Dec. 11, 2024.

[165] Ken Ip, *Greater Bay Area—China's Path to Silicon Valley 2.0?* China Daily (October 13, 2023), https://www.chinadaily.com.cn/a/202310/13/WS6528ec7ba31090682a5e86aa.html (last visited Aug. 1, 2024).

[166] Yuxuan Ma, Lei Wang, Di Hu, Yaoqing Ge, Junzhu Zuo and Tian Lan, *Analysis of Spatial Patterns of Technological Innovation Capability Based on Patent Data in Jiangsu Province, China*, 10.1 HUMANITIES AND SOC. SCI. COM. 1 (2023).

[167] Decision of the Yangzhong Public Security Bureau on Administrative Penalty for Fan Moumou (范某某) (2023) No. 279.

[168] *Official Website of the CAC, The Decision of the CAC to Impose Administrative Penalties Related to Cybersecurity Review on DiDi Global Co., Ltd. According to Law*, (July 21, 2022), https://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm (last visited Aug. 1, 2024).

[169] Official website of the CAC, *The Decision of the CAC to Impose Administrative Penalties Related to Cybersecurity Review on DiDi Global Co., Ltd. According to Law*, (July 21, 2022), https://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm (last visited Aug. 1, 2024).

Table 5: Data Processor Categories

Category of Data Processors	Number of Cases	Percentage
Limited Liability Company	34	66.7%
Joint Stock Company	2	3.9%
Individual Industrial and Commercial Households	6	11.7%
Unknown	9	17.7%
Total	51	100%

Table 5 shows the categories of the punished data processors. The majority were limited liability company data processors (66.7%) such as CNKI.[170] Joint stock company data processors has only two cases. In China, the average size and capitalization of limited liability companies is usually much smaller than that of joint stock companies.[171] This indicates that although the main target of the 2021 PIPL regulation is VLOPs, the most law enforcement resources have been occupied by small personal information processors (small and medium-sized enterprises). Only a very small number of VLOPs such as DiDi were punished. This indicates that VLOPs were rarely sanctioned due to their influences on the local governments and local protectionism.[172]

5. Penalty Category

Table 6: Penalty Category

Category of Penalty	Number of Cases	Percentage
Warning	48	60%

[170] Official website of the CAC, *The Decision of the CAC to Impose Administrative Penalties Related to Cybersecurity Review on CNKI According to Law*, (Sept. 6, 2023), https://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm (last visited Aug. 1, 2024).

[171] This is because China's Company Law provides a much higher threshold for the establishment of joint stock companies. The companies that have the largest capitalization in China are mostly listed companies (a kind of joint stock company). *See* Marcus Lu, *Ranked: The 20 Top Chinese Stocks by Market Cap, and Performance YTD*, (Mar. 18, 2024), https://www.visualcapitalist.com/ranked-the-20-top-chinese-stocks-by-market-cap-and-performance-ytd/, VISUAL CAPITALIST (last visited Aug. 1, 2024).

[172] For instance, Tencent, a VLOP domiciled in Nanshan District of Shenzhen, won over ninety percent of the cases in Shenzhen's local courts between 2018 and 2020. *See* Zhenhuan Lei & Yishuang Li, *Making Local Courts Work: The Judicial Recentralization Reform and Local Protectionism in China*, https://nsd.pku.edu.cn/docs/20221003222234994110.pdf (last visited Aug. 1, 2024).

Order to Make Corrections	17	21.25%
Order to Suspend Production and Business Operations	11	13.75%
Fine (8.026 billion yuan for DiDi, 50 million yuan for CNKI, 30,000 yuan for Fan Moumou)	3	3.75%
Confiscation of Illegal Gains (5,050 yuan for Fan Moumou)	2	1.25%
Total	81	100%

Table 6 shows that the main form of administrative penalty is a warning, which accounts for sixty percent of penalties. This was followed by orders to make corrections and orders to suspend production and business, reflecting regulators' cautious regulatory attitude.

Fines and confiscation of illegal gains were conservatively used (only five cases), indicating that the level of administrative punishment was relatively light. For example, the regulators only imposed fines in three cases, namely DiDi (8.026 billion yuan),[173] CNKI (50 million yuan),[174] and Fan Moumou (30,000 yuan).[175] Confiscation of illegal gains only has two cases.[176] This shows that the fines were mainly made by the CAC in very rare situations against famous VLOPs such as DiDi.[177]

B. *Enforcement by the MIIT*

In addition to the traditional administrative penalty cases by the CAC and other agencies, the MIIT regularly released lists of apps that

[173] Official website of the CAC, *The Decision of the CAC to Impose Administrative Penalties Related to Cybersecurity Review on DiDi Global Co., Ltd. According to Law* (July 21, 2022), https://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm (last visited Aug. 1, 2024).

[174] Official website of the CAC, *The Decision of the CAC to Impose Administrative Penalties Related to Cybersecurity Review on CNKI According to Law* (Sept. 6, 2023), https://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm (last visited Aug. 1, 2024).

[175] *Decision of the Yangzhong Public Security Bureau on Administrative Penalty for Fan Moumou* (范某某) (2023) No. 279.

[176] A typical case is the case of Fan Moumou, where 5,050 yuan of illegal gains was confiscated. *See Decision of the Yangzhong Public Security Bureau on Administrative Penalty for Fan Moumou* (范某某) (2023) No. 279.

[177] These kinds of VLOP cases are often well-known cases that attracted nationwide focus. *See* official website of the CAC, *The Decision of the CAC to Impose Administrative Penalties Related to Cybersecurity Review on DiDi Global Co., Ltd. According to Law* (July 21, 2022), https://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm (last visited Aug. 1, 2024).

conducted personal data misconduct.[178] Through this mechanism, the MIIT can order data processors to make corrections and impose reputational sanctions for data processors. This author searched all the lists and focuses on data processors' violations of personal data protection obligations. After searching and screening, this author found 1,233 cases involving personal information infringement by data processors via apps.

1. Distribution of Cases by Time

Table 7: Distribution of Cases by Time

Year	Number of Cases	Percentage
2019	23	1.8%
2020	396	32.1%
2021	486	39.4%
2022	188	15.3%
2023	128	10.4%
2024	12	1%
Total	1233	100%

Table 7 shows the time distribution of the MIIT cases. With the rapid development of the digital economy, the number of online personal information infringement cases involving apps has increased rapidly from 2019 to 2021. For example, in 2019, QQ Reading collected users' personal information without authorization.[179] On November 1, 2021, the PIPL was officially implemented, and the state strengthened the prevention and punishment of app infringement of personal data. Since then, the total number of cases reached a peak before it was stabilized to a certain extent.

2. Identity of App Developers

Table 8: Identity of App Developers

Identity of App Developers	Number of Cases	Percentage
Natural Person	1	0.08%

[178] As for the database of the cases, *see* official website of the MIIT, https://www.miit.gov.cn/ (last visited Aug. 1, 2024).

[179] Official website of the MIIT, *Announcement on App Infringement of User Rights and Interests (First Batch)* (Dec. 20, 2019), https://www.gov.cn/xinwen/2019-12/20/content_5462577.htm (last visited Aug. 1, 2024).

Enterprise	1,231	99.84%
Unknown	1	0.08%
Total	1,233	100%

Table 8 shows the identity of the app developer. App developers are mainly enterprises, accounting for 99.92% of all cases. In only one case, the app was developed by a natural person. In the case of Fitness Expert made by Liu Hongwei, the app was involved in illegal collection of personal information.[180] This shows that compared with natural persons, app development enterprises have more human and financial resources and are the focus of supervision by regulators.

3. Geographical Distribution of App Developers

Table 9: Geographical Distribution of App Developers

Province	Number of Cases	Percentage
Beijing	394	31.9%
Guangdong	245	19.9%
Shanghai	191	15.5%
Zhejiang	91	7.4%
Fujian	40	3.2%
Jiangsu	40	3.2%
Sichuan	35	2.8%
Hubei	31	2.5%
Hunan	29	2.4%
Anhui	20	1.6%
Chongqing	18	1.5%
Tianjin	16	1.3%
Shandong	15	1.2%
Hainan	11	0.9%
Other 15 provinces (Case number below 10)	55	4.5%
Unknown	2	0.2%
Total	1233	100%

[180] Official Website of the MIIT, *Announcement on App Infringement of User Rights and Interests (Sixth Batch of 2020)* (Dec. 6, 2020), https://www.gov.cn/xinwen/2020-12/06/content_5567292.htm (last visited Aug. 1, 2024).

Table 9 shows the geographical distribution of app developers. App developers are mainly distributed in Beijing, Guangdong, Shanghai and Zhejiang (together accounting for seventy-five percent of all cases). The number of App developers located in Beijing, Guangdong and Shanghai exceeded one hundred each, and Zhejiang had ninety-one. Not surprisingly, these are the regions with the highest economic level, the most developed private sector, and the most VLOPs in China.[181] For example, Beijing has Baidu, Guangdong has Tencent, and Zhejiang has Alibaba.[182] Smaller app developers tend to cluster in cities where these big tech companies are located and facilitate the formation of a healthy, innovative technological ecosystem.[183] In contrast, the western and northern regions, which are dominated by state-owned enterprises and heavy industry, have seen a small number of cases.[184] Fifteen provinces, such as Liaoning, had fewer than ten cases each.[185]

4. Downloading Platform of App

Table 10: Downloading Platform of App

Downloading Platform of App	Number of Cases	Percentage
App Stores	1083	87.83%
Official Websites and Mini Phone Programs	141	11.44%
Other Websites	9	0.73%
Total	1233	100%

Table 10 shows where the relevant apps were downloaded. Apps that infringe on users' personal data mainly come from software stores such

[181] PwC China: Chinese Cities of Opportunity 2023, https://www.pwccn.com/en/research-and-insights/chinese-cities-of-opportunities-2023-report.html (last visited Aug. 1, 2024).

[182] These three big tech companies are collectively referred to as "BAT" in the Chinese market.

[183] Wu, Yue, et al., *The Correlation Between the Jobs-Housing Relationship and the Innovative Development of Sci-Tech Parks in New Urban Districts: A Case Study of the Hangzhou West Hi-Tech Corridor in China*, 9.12 ISPRS INT'L J. OF GEO-INFO. 762 (2020).

[184] Zhong Nan, *Northeast SOEs Raring to Prove Their Mettle*, CHINA DAILY (Oct. 19, 2023), https://www.chinadaily.com.cn/a/202310/19/WS65308810a31090682a5e96dd.html (last visited Aug. 1, 2024).

[185] FORBES, *China Has Its Own Rust Belt, and It's Getting Left Behind as the Country Prospers* (July 14, 2017), https://www.forbes.com/sites/outofasia/2017/07/14/dongbei-china-rust-belt/ (last visited Aug. 1, 2024).

as Ying Yong Bao (应用宝), accounting for more than eighty percent.[186] This shows that app downloads are mainly from mainstream software app stores operated by VLOPs, such as Ying Yong Bao managed by Tencent.[187] This is similar to the U.S., where people primarily download apps from app stores managed by big tech companies such as Apple. However, the app store is rarely held accountable. In 2013, a U.S. federal court held that an app store is not liable for legal violations by third-party apps.[188]

C. Regulatory Cooperation Under the Twin Peaks Model

1. Categories of Violations Punished by the CAC

Table 11: Categories of Violations Punished by the CAC

Category of Violation	Number of Cases	Percentage
1. General Violation of Personal Information Security Protection in Computer Systems	20	27%
2. Rules for Collection and Use Are Not Disclosed or Expressed	18	24.3%
3. Collecting Personal Information Without Consent	15	20.3%
4. Encryption and De-identification Are Not Adopted	9	12.2%
5. The Validity and Integrity of the Application Signature or Certificate Have Not Been Verified	5	6.8%
6. Risk of Arbitrary Backup, Tampering, and Repackaging of App Data	4	5.4%
7. Collecting Personal Information in Violation of the Principle of Necessity	2	2.7%
8. Failing to Provide Account Cancellation Function or Failing to	1	1.3%

[186] Official Website of the MIIT, *Announcement on App Infringement of User Rights and Interests (Sixth Batch of 2020)* (Dec. 6, 2020), https://www.gov.cn/xinwen/2020-12/06/content_5567292.htm (last visited Aug. 1, 2024).

[187] Official website of Ying Yong Bao, *Download the Latest and Hottest Mobile App Games in the Network*, https://sj.qq.com/ (last visited Aug. 1, 2024).

[188] Samuel M. Roth, *Data Snatchers: Analyzing TikTok's Collection of Children's Data and Its Compliance with Modern Data Privacy Regulations*, 22 J. HIGH TECH. L. 1, 32 (2021).

Delete Personal Information in Time After Cancellation		
Total	74	100%

Table 11 shows the specific categories of violations by data processors punished by the CAC. Multiple violations may be involved in a single case. There are three categories of violations with the largest number of cases. The first involves general violations of personal information security protection in computer systems (twenty cases). This is a typical catch-all provision. For example, Shenzhen Gold Investment Co., Ltd. did not verify the SSL certificate, which is a general violation of the personal information security of the computer system.[189] The second category entails cases when rules for the collection and use of personal information are not disclosed or expressed (eighteen cases). The third involves the collection of personal information without consent (fifteen cases). For example, CNKI engaged in the act of disclosing personal privacy such as collecting personal information without consent, failing to disclose or express the collection and use rules.[190] In contrast, the right to be forgotten seems to have been forgotten by regulators. In only one case (CNKI), the CAC punished the failure to delete personal information in a timely manner.[191]

2. Categories of Violation Punished by the MIIT

Table 12: Categories of Violation Punished by the MIIT

Category of Violation	Number of Cases	Percentage
1. Illegal Collection of Personal Information	949	62.6%
2. Illegal Use of Personal Information	245	16.2%
3. Excessive Collection of Personal Information	206	13.6%
4. Collecting Personal Information without Permission	82	5.4%

[189] Decision of the Futian Branch of Shenzhen Public Security Bureau on Administrative Penalty for Shenzhen Huangjin Touzi Youxian Gongsi (深圳黄金投资有限公司) [Shenzhen Gold Investment Co., Ltd] (2023) No. 33021.

[190] Official website of the CAC, *The Decision of the CAC to Impose Administrative Penalties Related to Cybersecurity Review on CNKI According to Law* (Sept. 6, 2023), https://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm (last visited Aug. 1, 2024).

[191] *Id.*

5. Inadequate Express Notification of Personal Information Collection	17	1.1%
6. Illegal Use of Personal Information to Carry out Automated Decision-Making	6	0.4%
7. Deceiving and Misleading Users to Provide Personal Information	4	0.26%
8. Illegally Transmitting Personal Information	3	0.19%
9. Forced Collection of Nonessential Personal Information	3	0.19%
10. Illegal Use of Third-Party Services	1	0.06%
Total	1516	100%

Table 12 shows the ten categories of personal information violations by apps punished by the MIIT. They can be summarized into three sub-categories: (1) illegal collection, use, processing, and transmission of others' personal information; (2) illegal trade, provision, or disclosure of others' personal information; and (3) engagement in personal information processing activities that endanger national security and public interests.[192] It is worth noting that MIIT law enforcement activities have a clear focus, which is on the illegal collection of personal information (949 cases, or 62.6%). Most cases involved the illegal or excessive collection and use of personal information, which shows app developers often neglected users' personal data rights.

It is interesting to find that there were only three cases of illegal transmission of personal information. This may be explained by the fact that many data processors such as VLOPs have established entrustment mechanisms that comply with legal provisions and are able to avoid legal risks.[193] The trustee who accepts the commission to process personal information shall take necessary measures to ensure the security of the personal information being processed and assist the data processor in fulfilling its obligations.[194]

[192] Article 10 of the 2021 PIPL.

[193] For instance, Xiaomi has established an Information Security and Privacy Committee. *See* Guo Pengqi, *Xiaomi Emphasizes the Importance of Security and Privacy, Focuses on IoT Security, and Creates Reliable AIoT Products* (Nov. 10, 2020), https://finance.sina.cn/2020-11-10/detail-iiznctke0682988.d.html, Sina (last visited Aug. 1, 2024).

[194] Article 59 of the 2021 PIPL.

V. COMPARATIVE ANALYSES AND POLICY SUGGESTIONS

A. *Divergent Institutional Structures*

Since the opening-up of its economy, China has conducted many legal transplantation projects based on legal models from the West, especially the U.S. and EU.[195] This Article compares the personal data protection laws of China, the EU, and U.S. (California). They have many convergences and even bigger divergences in crucial areas such as the structure of regulatory institutions and administrative penalties.

1. Cross-Jurisdictional Comparison

The U.S. has adopted a regulatory model dominated by state laws. To date, there has been no centralized data protection regulator on the federal level. The Federal Trade Commission (FTC) has broad powers to investigate and prevent unfair methods of competition.[196] However, the FTC is viewed as ill-equipped to find out what companies like Google and Facebook are doing behind the scenes. Also, it is short of sufficient enforcement power.[197] California's CCPA has inspired other U.S. states such as Virginia and Colorado to enact comprehensive data privacy statutes.[198] The regulator in California is the attorney general or the California Privacy Protection Agency.

The EU has adopted a model of decentralized regulation in which the EU and member states share regulatory power and work together. The GDPR requires member states to establish Data Protection Authorities (DPA) and has created the European Data Protection Board (EDPB).[199] Data subjects whose rights are violated can appeal to the supervisory authority of member states,[200] who can impose administrative fines.[201] If the data processors disagree with the ruling of the regulatory authority, they can exercise the right of judicial relief to the local court.[202] In 2022,

[195] For more discussions on features of China's legal transplantation of U.S. laws, *see* Robin Hui Huang, Charles Chao Wang, *The Mandatory Bid Rule Under China's Takeover Law: A Comparative and Empirical Perspective*, 53(2) INT'L LAW. 195 (2020).

[196] Section 5(a) of the FTC Act.

[197] Peter Maass, *Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless*, WIRED (June 28, 2012), https://www.wired.com/2012/06/ftc-fail/ (last visited Aug. 1, 2024).

[198] Data Protection Laws and Regulations Report 2023-2024 USA, https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa (last visited Aug. 1, 2024).

[199] Article 68 of the 2016 GDPR.

[200] Article 77 of the 2016 GDPR.

[201] Article 83 of the 2016 GDPR.

[202] Article 78 of the 2016 GDPR.

a new pan-European supervisory architecture was established by the DSA. Enforcement powers are divided between the European Commission and member states.[203] The European Commission is the competent authority for supervising the platforms in close cooperation with the Digital Services Coordinators established by the DSA.[204] These national authorities, which are responsible for the supervision of smaller platforms, needed to be established by EU member states before February 17, 2024.[205]

Unlike the U.S. and the EU, China has adopted a two-tier enforcement model. At the state level, China has adopted a distinctive twin peaks model.[206] The CAC and the MIIT share the regulatory powers and assume supplementary roles. At the local level, China decentralized regulatory powers to local governmental agencies. The CAC relies on local government agencies (public security bureaus of municipal and district/county levels) to impose administrative sanctions on local data processors.[207] This decentralization arrangement is reasonable, because unlike more sophisticated governmental agencies like the CSRC, the CAC does not have enough local branches to impose administrative sanctions.[208] As a government agency with a short history, the CAC faces a serious shortage of human and financial resources.[209] Therefore, it is

[203] Article 56 of the 2022 DSA.

[204] *Algorithmic Transparency*, European Commission, https://algorithmic-transparency.ec.europa.eu/index_en.

[205] European Commission Press Release, *Digital Services Act: Commission Designates First Set of Very Large Online Platforms and Search Engines* (Apr. 25, 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413 (last visited Aug. 1, 2024).

[206] The CAC and the MIIT form the twin peaks of regulators. *See China's CAC and MIIT Undertake Parallel Consultations on Draft Measures for Cyber Incident Reporting*, (Jan. 24, 2024), https://www.hoganlovells.com/en/publications/chinas-cac-and-miit-undertake-parallel-consultations-on-draft-measures-for-cyber-incident-reporting#:~:text=The%20CAC%20is%20China's%20cyber,the%20technology%20and%20telecommunications%20industries, HOGAN LOVELLS (last visited Aug. 1, 2024).

[207] This can be seen from the case studies of this Article, which show that the majority of local cases were decided by local public security bureaus.

[208] The enforcement of securities laws has been undertaken by not only the CSRC, but also the CSRC's local branches. *See* Robin Hui Huang, Charles Chao Wang, *The Law and Practice of Substantial Shareholding Disclosure in China: Comparative Perspectives and Recent Developments*, 48 SEC. REGUL. L.J. 3 (2020).

[209] Similarly, the CSRC has the problem of human and financial resource shortages. *See* Fa Chen, Lijun Zhao, *The Comprehensive Implementation of the Registration-Based System of IPO Regulation in China: Practice, Progress, Problems and Prospects*, 32(1) ASIA PACIFIC L. REV. 1 (2024).

efficient for China to delegate powers to the local public security bureaus which have more law enforcement resources at the grass-roots level.

The law enforcement styles of the CAC and the MIIT have similarities, such as a common focus on regulating the collection activities of personal information by data processors.[210] However, CAC law enforcement focuses on the invocation of catch-all provisions to punish general violations of personal information security of the computer system.[211] The MIIT focuses on the supervision of app developers, so its law enforcement is more concentrated on data processors' specific misconduct. More than ninety percent of the MIIT's cases involved the illegal or excessive collection and use of personal information.[212]

2. Contextual Analysis

This Article argues that one of the advantages of the U.S. and EU regulatory models is that they are relatively decentralized, and each jurisdiction (U.S. states or EU member states) can enforce the law according to its own actual situation. As of April 1, 2024, the EU member states with the highest number of enforcement cases are Spain (827 cases), Italy (353 cases), Germany (176 cases), and Romania (174 cases).[213] However, this is also prone to regulatory arbitrage and multiple penalty problems. For instance, TikTok has been investigated in France, the United Kingdom, the Netherlands, and Italy for violation of GDPR.[214]

China's two-tier regulatory model has certain advantages. Under the twin peaks model, the CAC focuses on imposing administrative penalties on data processors, while the MIIT focuses on the regulation of app developers. The sharing of regulatory functions by the CAC, the MIIT, and other agencies can achieve an effect of regulatory cooperation and target coordination where regulatory arbitrage is not easy to occur.

However, China's decentralization at the local level may lead to the uneven enforcement standards between the central and local levels. For example, in the DiDi case, the CAC issued a huge fine of 8.026 billion

[210] Chinese companies like TikTok often obtain consent by use, only allowing users to submit requests to uncover the collected data. *See* TikTok, *Privacy Policy* (Mar 22, 2024), https://www.tiktok.com/legal/privacy-policy-us?lang=en (last visited Aug. 1, 2024).

[211] *Id.*

[212] The enforcement rules formulated by the MIIT list the illegal collection and use of personal information by apps. *See* Article 1 of the 2019 App Identifying Methods Draft.

[213] GDPR Enforcement Tracker, *List of GDPR Fines*, https://www.enforcementtracker.com/?insights (last visited Aug. 1, 2024).

[214] Samuel M. Roth, *Data Snatchers: Analyzing TikTok's Collection of Children's Data and Its Compliance with Modern Data Privacy Regulations*, 22 J. HIGH TECH. L. 1, 32 (2021).

yuan, which is never seen in local cases.[215] Therefore, China should learn from the EU model of decentralized regulation, which features a division of power and cooperation between the EU and its member states.[216] The Digital Services Coordinator is supposed to be an independent body.[217] They must exercise power in conformity with the EU Charter of Rights and subject to safeguards in national law.[218] In addition, the European Commission may issue guidelines that present best practices and recommend possible measures.[219]

B. Divergent Administrative Penalties

1. Cross-Jurisdictional Comparison

This Article makes a comparison between administrative penalties of China, the EU, and the US. There are many differences that can be observed.

First, the frequencies of administrative penalties are different. As of April 1, 2024, there are 1,284 cases of administrative penalty in China (51 CAC cases and 1,233 MIIT cases), while the number of cases in the EU is very large (2,279 cases).[220] This shows that EU member states have rich experiences in public enforcement of data protection laws. China's legal regulation of data processors previously subordinated personal data protection to network infrastructure construction, platform economy development, and cybersecurity interests for a long time after China's accession to the WTO. Since the enactment of the 2021 PIPL, personal data protection has been an important issue with a soaring number of cases. However, most cases were handled by the MIIT, and it remains to be seen whether the CAC will reinforce the regulation on data protection in the future.

[215] Official Website of the CAC, *The Decision of the CAC to Impose Administrative Penalties Related to Cybersecurity Review on DiDi Global Co., Ltd. According to Law* (July 21, 2022), https://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm (last visited Aug. 1, 2024).

[216] Some scholars argued that the U.S. should learn from the EU and consider passing a federal data privacy law. *See* Vanessa Perumal, *The Future of US Data Privacy: Lessons from the GDPR and State Legislation*, 12 NOTRE DAME J. INT'L COMP. L. 99 (2022); Moises Barrio Andres, *The Regulation of Data Protection Law in the United States: Towards an American GDPR*, 14 CUADERNOS DERECHO TRANSNACIONAL 186 (2022).

[217] Article 41 (2) of the 2022 DSA.

[218] Article 51 (6) of the 2022 DSA.

[219] Article 35 (2) of the 2022 DSA.

[220] GDPR Enforcement Tracker, *List of GDPR Fines*, https://www.enforcementtracker.com/?insights (last visited Aug. 1, 2024).

Second, the emphases of administrative penalties are different. The CAC enforcement mainly focuses on specific illegal acts, among which the illegal collection of personal information is the most common misconduct. In the EU, the biggest number of fines have been imposed on two categories of violations: non-compliance with general data processing principles and insufficient legal basis for data processing.[221] This means EU regulators attach great importance to applying basic principles in broad terms. Some EU norms regulating platforms do not contain detailed substantive criteria. For example, the DSA does not talk about what additional requirements a social media platform must enforce regarding offensive speech in addition to the minimum requirements. [222]

Third, the vertical division of regulatory powers is different. First, at the federal or EU level, the U.S. and the EU have adopted decentralized regulatory models where there is no CAC-style regulator.[223] At the state level, China has adopted a twin peaks model, with the CAC and the MIIT being the major regulators.[224] Second, at the local level, the EU's administrative penalty cases are highly dispersed.[225] Each member state has a large or small number of penalty cases.[226] China has decentralized regulatory powers to local governmental agencies (municipal and district/county levels), especially those from Jiangsu province and Guangdong province.[227] With insufficient law enforcement experience and resources, it is natural for the Chinese government to coordinate its regulatory efforts on data processors that are located in developed provinces where technology companies are concentrated.

[221] *Id.*

[222] Zsolt Zodi, *Characteristics of the European Platform Regulation: Platform Law and User Protection*, 7 PUB. GOVERNANCE, ADMIN. & FIN. L. REV. 91 (2022).

[223] The FTC is not a CAC-style regulator that specifically deals with personal data breaches with delegated statutory powers.

[224] *China's CAC and MIIT Undertake Parallel Consultations on Draft Measures for Cyber Incident Reporting*, (Jan. 24, 2024), https://www.hoganlovells.com/en/publications/chinas-cac-and-miit-undertake-parallel-consultations-on-draft-measures-for-cyber-incident-reporting#:~:text=The%20CAC%20is%20China's%20cyber,the%20technology%20and%20telecommunications%20industries, HOGAN LOVELLS (last visited Aug. 1, 2024).

[225] GDPR Enforcement Tracker, *List of GDPR Fines*, https://www.enforcementtracker.com/?insights (last visited Aug. 1, 2024).

[226] For instance, Ireland has imposed twenty-nine fines of €3,256,363,400 in total, while Cyprus has imposed forty-four fines of €1,432,500 in total. *See* GDPR Enforcement Tracker, *List of GDPR Fines*, https://www.enforcementtracker.com/?insights (last visited Aug. 1, 2024).

[227] This can be seen from the case studies of this Article, which shows that the majority of cases were decided by local agencies.

Fourth, the amount and frequency of administrative fines are different. Compared with China and California, the EU's fines are much greater and more frequently imposed. The statutory fine is twenty million euros, or four percent of total global turnover of the preceding fiscal year.[228] In practice, the EU regulators have frequently imposed fines based on GDPR.[229] Amazon faces the biggest ever EU fine (746 million-euros, or $888 million) for a data privacy breach by the Luxembourg data protection authority.[230] The biggest fine to date was imposed on Google in France (fifty million euros).[231] By comparison, California's fine is capped at $7,500.[232] In China, the main form of punishment for data processors is a warning and an order to make corrections, reflecting regulators' cautious approach to applying more serious penalties such as fines. The regulators imposed fines in very few cases and the amounts were mostly low (the maximum is 8.026 billion yuan). The fines have mainly been imposed on VLOPs such as DiDi, in high-profile cases that attracted market attention.[233] Compared with China and the U.S., the EU has much harsher monetary sanctions on data processors.

Fifth, the exemption mechanisms for administrative penalties are different. In China, the exemption grounds of personal data protection include: (1) personal data processing by natural persons for personal or family affairs and (2) personal data processing in statistical and archival management activities organized by governments at all levels.[234] In the EU, the DSA provided detailed exemption grounds in Articles 4, 5, and 6. In summary, it seems that China's exemption mechanism mainly

[228] Article 83 of the 2016 GDPR.

[229] GDPR Enforcement Tracker, *List of GDPR Fines*, https://www.enforcementtracker.com/?insights (last visited Aug. 1, 2024).

[230] Stephanie Bodoni, *Amazon Given Record $888 Million EU Fine for Data Privacy Breach*, BLOOMBERG NEWS (July 30, 2021), https://www.bnnbloomberg.ca/amazon-given-record-888-million-eu-fine-for-data-privacy-breach-1.1634824 (last visited Aug. 1, 2024).

[231] European Data Protection Board, *The CNIL's Restricted Committee Imposes A Financial Penalty of 50 Million Euros Against GOOGLE LLC* (Jan. 21, 2019), https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en (last visited Aug. 1, 2024).

[232] Article 1798.155 of the 2018 CCPA.

[233] Official Website of the CAC, *The Decision of the CAC to Impose Administrative Penalties Related to Cybersecurity Review on DiDi Global Co., Ltd. According to Law* (July 21, 2022), https://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm (last visited Aug 1, 2024).

[234] Article 72 of the 2021 PIPL.

protects the interests of government agencies, while the EU exemption rules focus on balancing the interests of users and platforms.[235]

2. Contextual Analysis

This Article argues that the main reason for these divergences is that they have different political and economic contexts.[236] In the EU, American tech giants such as GAFAM (Google, Apple, Facebook, Amazon and Microsoft) have great influences, while local European platforms are relatively weak. As a result, EU regulators often attempt to curb foreign big tech firms to protect local platforms.[237] The companies that received the biggest fines in the EU are Meta Platforms (particularly its platforms Facebook and WhatsApp), Amazon, TikTok, and Google.[238]

In China, the government's national strategy is to facilitate the development of VLOPs like BATJ and Tiktok to fulfill the country's global ambitions.[239] It is natural for the government to relieve data processors of too much compliance burden. For example, law enforcement has been used mainly to target small personal information processors (small and medium-sized enterprises), while the proportion of VLOP cases has been low.[240] Fines were very rarely imposed.[241] In only one case, the CAC punished the failure to delete personal information,[242]

[235] As for the discussions on exemptions, *see* Miriam C. Buiten, *The Digital Services Act from Intermediary Liability to Platform Regulation*, 12 J. INTELL. PROP. INFO. TECH. & ELEC. COM. L. 361 (2021).

[236] Although China transplanted a lot of laws from Europe and the U.S., the local political economy is more important than the legal origin in explaining the Chinese law and practice. *See* Guanghua Yu & Shao Li, *Against Legal Origin: Of Ownership Concentration and Disclosure*, 7.2 J. OF CORP. L. STUDIES 285 (2007).

[237] Samuel Stolton, *Apple, Google Defeats to Fuel EU's Crackdown on Big Tech,* https://www.bnnbloomberg.ca/business/company-news/2024/09/10/apple-google-defeats-to-fuel-eus-crackdown-on-big-tech/, BNN Bloomberg (Sept. 10, 2024) (last visited Aug. 1, 2024).

[238] GDPR Enforcement Tracker, *List of GDPR Fines*, https://www.enforcementtracker.com/?insights (last visited Aug. 1, 2024).

[239] TikTok is the fastest growing app in history. *See* Brad Koyak, *Meet TikTok: The Fastest Growing App in History*, LAURUS COLL., https://lauruscollege.edu/meet-tiktok/ (last visited Aug. 1, 2024); As for China's national strategy of developing national champions, *see* Li-Wen Lin and Curtis J Milhaupt, *We Are the (National) Champions: Understanding the Mechanisms of State Capitalism in China*, 65 (4) STAN. L. REV. 697 (2013).

[240] Li-Wen Lin and Curtis J Milhaupt, *We Are the (National) Champions: Understanding the Mechanisms of State Capitalism in China*, 65 (4) STAN. L. REV. 697 (2013).

[241] *Id.*

[242] Official Website of the CAC, *The Decision of the CAC to Impose Administrative Penalties Related to Cybersecurity Review on CNKI According to Law* (Sept. 6, 2023), https://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm (last visited Aug. 1, 2024).

which shows the right to be forgotten seems to have been forgotten by the regulator.

This relaxed law enforcement will enable Chinese digital platforms to acquire more data resources to fully develop big data and achieve global competitive advantage over American VLOPs in the Sino-U.S. tech war. Therefore, China will not wholly adopt the stringent EU model of harsh penalty in the future. Instead, China will converge with the U.S. by maintaining the low monetary sanctions, thus achieving a balance between data protection regulatory goals and national development agendas. To this end, it is recommended that China improve the exemption mechanism of personal data breaches to prevent technology companies from taking excessive liability risks.

C. Balancing Public Interests Protection

1. Review of Sensitive Data

China's obligation to protect personal data must be reconciled with the protection of the public interests. Public interests are reflected in the processing of sensitive data. Under the 2021 PIPL, "sensitive personal information" refers to personal information that, once disclosed or illegally used, may easily lead to infringement on the personal dignity of natural persons or harm to their personal and property safety. The scope of "sensitive personal information" includes biometric identification, religious belief, specific identity, medical and health care, financial accounts, whereabouts, and other information, as well as the personal information of minors under the age of fourteen. The additional requirements to process sensitive personal information are: (1) a specific purpose and sufficient necessity; (2) strict protection measures; (3) individual separate consent; and (4) written consent under legal circumstances.[243]

In the EU, Recital of the GDPR explains the public interests in different scenarios. Data collection activities must be compatible with the purposes, accommodating data processing activities that are necessary to perform for public interests.[244] Where adequate safeguards are in place, the fundamental rights of data subjects are restricted for specific purposes, such as public health.[245] Sensitive data should only be processed if

[243] Articles 28, 29 of the 2021 PIPL.

[244] Paragraph 50, Recital of the 2016 GDPR.

[245] Paragraph 52, Recital of the 2016 GDPR.

necessary for public interests in the areas such as public health.[246] Scholars divide public interest into general public interests and important public interests. For important public interests, data processing will be regarded as legal even if it involves the processing of sensitive data.[247]

2. Ideological Censorship and National Security Review

China's "public interests" are embodied in the ideological censorship and national security reviews conducted by data processors on users' information. Chinese data processors have the obligation to manage the information released by users. If it discovers any information prohibited by law from being published or transmitted, the data processor shall immediately stop transmitting such information, take disposal measures such as elimination, keep relevant records, and report it to the relevant competent authorities.[248] The obligation to review personal information requires that data processors do not produce, copy, publish, or disseminate certain information, including statements: (1) opposing the basic principles of the Constitution; (2) endangering national security; (3) harming national honor and interests; (4) inciting ethnic hatred or ethnic discrimination; or (5) preaching evil religions and feudal superstition.[249]

In addition, Chinese regulators make extensive use of catch-all provisions to exercise discretionary powers to implement the Chinese government's understanding of "national security." For example, in the DiDi case, the CAC imposed huge fines. This is because DiDi not only infringed on users' personal data, but also endangered China's national security.[250] Against the backdrop of the Sino-U.S. trade and technology wars, DiDi's plan to get listed in the U.S. stock market could potentially jeopardize China's data security and global strategy by disclosing sensitive big data to U.S. regulators.[251]

[246] Paragraph 53, Recital of the 2016 GDPR.

[247] Meszatos J. & Ho C., *Big Data and Scientific Research: The Secondary Use of Personal Data Under the Research Exemption in the GDPR*, 59(4) HUNGARIAN J. OF LEGAL STUDIES 403 (2018).

[248] Article 5 of the 2012 NPC Decision.

[249] Article 57 of the 2016 Telecommunications Regulation.

[250] Ruoxi Wang, Chi Zhang and Yaxiong Lei, *Justifying a Privacy Guardian in Discourse and Behaviour: The People's Republic of China's Strategic Framing in Data Governance*, 59(2) INT'L SPECTATOR 58 (2024).

[251] Julie Zhu, Yingzhi Yang & Kane Wu, *China Fines DiDi $1.2 bln but Outlook Clouded by App Relaunch Uncertainty*, REUTERS, https://www.reuters.com/technology/china-fines-didi-global-12-bln-violating-data-security-laws-2022-07-21/ (last visited Aug. 1, 2024); Digichina,

The findings above agree with people's concern that when the law of the West was transplanted to authoritarian countries, the government of the recipient country might enlarge their control over the dissemination of information. In the process, speech critical of the government may be targeted.[252] Indeed, the Chinese government has a final say on whether the personal information on a digital platform is in violation of China's national security and ideological standards.[253]

3. Automated Decision-Making

To protect public interests, automated decision-making must be regulated. Improving the transparency of data collection and processing will encourage the artificial intelligence industry to take the initiative to avoid violating society's privacy expectations.[254] According to the "privacy by design" theory, personal data protection should be the default setting of data processor's artificial intelligence products.[255]

The 2021 PIPL stipulates that data processors using personal information to make automated decisions should ensure the transparency of decisions and the fairness and impartiality of results.[256] They should not implement unreasonable differential treatment for data subjects in terms of transaction prices and other transaction conditions.[257] Information push and commercial marketing to individuals through automated decision-making should also provide options that are not

Translation: *Chinese Authorities Announce $1.2B Fine in DiDi Case, Describe 'Despicable' Data Abuses*, https://digichina.stanford.edu/work/translation-chinese-authorities-announce-2b-fine-in-didi-case-describe-despicable-data-abuses/ (last visited Aug. 1, 2024).

[252] Anupam Chander, *When the Digital Services Act Goes Global*, 38 BERKELEY TECH. L.J. 1067 (2023).

[253] This indicates that foreign laws usually go through a totally different social network when transplanted into China. *See* David C. Donald, *Conceiving Corporate Governance for an Asian Environment*, 12(2) UNIV. OF PA. ASIAN L. REV. 88 (2016). A unique Chinese version of national security review can also be found in the screening of foreign investment in China, *see* Yuwen Li and Cheng Bian, *A New Dimension of Foreign Investment Law in China: Evolution and Impacts of the National Security Review System*, 24.2 ASIA PACIFIC L. REV. 149 (2016); Cheng Bian, *National Security Review of Foreign Investment in China*, 15 ERASMUS L. REV. 278 (2022).

[254] Shlomit Yanisky-Ravid & Sean K. Hallisey, *Equality and Privacy by Design: A New Model of Artificial Intelligence Data Transparency via Auditing, Certification, and Safe Harbor Regimes*, 46 FORDHAM URB. L.J. 428 (2019).

[255] Eric Everson, *Privacy by Design: Taking Ctrl of Big Data*, 65 CLEV. ST. L. REV. 27, 28 (2016).

[256] Article 24 of the 2021 PIPL.

[257] Automated decision-making refers to the activity of automatically analyzing and evaluating an individual's behavioral habits; interests; or economic, health, credit status, etc. through computer programs and decision making. *See* Article 73 of the 2021 PIPL.

specific to their personal characteristics, or provide individuals with convenient ways to refuse. If a decision is made by automated decision-making that has a significant impact on the data subject's rights, the data subject can request the data processor to explain it. The data subject has the right to reject the decision made by the data processor only by automated decision-making.[258]

These rules are forward-looking, but too general. In this regard, China should learn from the EU's experience in tackling specific problems of automated decision-making. Under the GDPR, data subjects shall not be subject to a decision based solely on automated processing.[259] The GDPR stipulates in detail the right of access,[260] right to restriction of processing,[261] and right to object[262] enjoyed by data subjects. Appropriate technical and procedural organizational measures should be implemented to ensure that data processing is performed in accordance with the GDPR standards.[263] The DSA prohibits any use of profiling to present targeted advertisements.[264] The European Commission launched the European Centre for Algorithmic Transparency (ECAT).[265] It will provide support with assessments as to whether the functioning of algorithms is in line with the risk management obligations.[266]

D. *Enhanced Regulation of Gatekeepers*

1. Taking VLOPs Seriously

In the field of data regulation, VLOPs have the power of gatekeepers.[267] Large platforms have a greater impact on personal

[258] Article 24 of the 2021 PIPL.

[259] Article 22 of the 2016 GDPR.

[260] Article 15 of the 2016 GDPR.

[261] Article 18 of the 2016 GDPR.

[262] Article 22 of the 2016 GDPR.

[263] Article 25 of the 2016 GDPR.

[264] *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act)*, 2022 O.J. (L 277) 1.

[265] Algorithmic Transparency, European Commission, https://algorithmic-transparency.ec.europa.eu/index_en (last visited Dec. 11, 2024).

[266] European Commission Press Release, *Digital Services Act: Commission Designates First Set of Very Large Online Platforms and Search Engines* (Apr. 25, 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413 (last visited Aug. 1, 2024).

[267] As for the gatekeeper mechanism in the DMA and the DSA, *see* Maria Luisa Chiarella, *Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment*, 9 ATHENS J. L. 33 (2023). As for the gatekeeper theory in corporate

information protection and should be the main target of regulation by regulators.[268] In terms of law on the book, China has set up the specific rules for VLOPs in the 2021 PIPL.[269] The above shows that apps that infringe on personal information in China mainly come from software stores such as App Treasure, accounting for more than eighty percent of cases.[270] However, in terms of law in action, the empirical research of this Article shows the opposite. It found that China's regulators mainly punish limited liability companies (accounting for 66.7%). The 2021 PIPL has been used mainly to target small personal information processors (small and medium-sized enterprises), while VLOPs were rarely sanctioned. This Article argues that Chinese law needs to strike a balance between encouraging the development of VLOPs and protecting personal data. In fact, the EU is also paying special attention to achieving this balance by issuing the initial list of services subject to the strictest rules under the DSA. These strictly regulated services are provided by VLOPs such as Facebook and TikTok.[271]

First, the standards for distinguishing VLOPs and small personal information processors should be improved. In the EU, the DSA stipulates that VLOPs and very large online search engines (VLOSEs) are those whose average users reach or exceed ten percent of the EU population.[272] To date, China does not have similarly clear rules. China should refer to the DSA standards to establish specific identification criteria for VLOPs and strengthen their supervision.

Second, China should learn from the DSA in designing new obligations for VLOPs, including more user empowerment, strong protection of minors, more diligent content moderation, less

governance, *see* John C. Coffee Jr, *Gatekeeper Failure and Reform: The Challenge of Fashioning Relevant Reforms*, 84 B.U. L.REV. 301 (2004).

[268] The move from an internet of decentralized networks to an internet of concentrated platforms been observed in the world. *See* Elettra Bietti, *A Genealogy of Digital Platform Regulation*, 7 GEO. L. TECH. REV. 1 (2023).

[269] Article 58 of the 2021 PIPL.

[270] Official Website of the MIIT, *Announcement on App Infringement of User Rights and Interests (Sixth Batch of 2020)* (Dec. 6, 2020), https://www.gov.cn/xinwen/2020-12/06/content_5567292.htm (last visited Aug. 1, 2024).

[271] European Commission Press Release, *Digital Services Act: Commission Designates First Set of Very Large Online Platforms and Search Engines* (Apr. 25, 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413 (last visited Aug. 1, 2024).

[272] Official Website of the EU, *Digital Services Act: Questions and Answers* (Apr. 3, 2024), https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers (last visited Aug. 1, 2024).

disinformation and more transparency and accountability.[273] Compared with ordinary data processors, VLOPs and VLOSEs have additional obligations, such as carrying out risk assessments and introducing risk mitigation measures.[274] For instance, gatekeeper platforms are forbidden to treat services and products offered by the gatekeeper itself more favorably in ranking than similar services or products offered by third parties on the gatekeeper's platform.[275]

2. Supervising Gatekeepers Independently

In order to strengthen the function of VLOPs as gatekeepers, Chinese law sets up mechanisms beyond the traditional corporate governance structure. First, a "personal information protection officer" (Geren Xinxi Baohu Fuzeren, or 个人信息保护负责人) should be designated by data processors that handle personal information up to a certain amount specified by the CAC. These data processors, very likely to be VLOPs, should disclose the officer's contact information and submit it to the regulator.[276] Second, if a data processor entrusts others to act as an agent for marketing and other services directly facing users, it shall supervise and manage the collection and use of users' personal information by the agent.[277] Third, Chinese law requires VLOPs to set up an independent organization composed mainly of external members to supervise and regularly issue social responsibility reports on personal data protection.[278]

The empirical research of this Article shows that most of those punished are organizations rather than natural persons. This means personal information protection officers are not being sanctioned. Its due supervisory function is questionable. It remains to be seen whether the functions of the personal information protection officer and the external

[273] *European Commission Press Release, Digital Services Act: Commission Designates First Set of Very Large Online Platforms and Search Engines* (Apr. 25, 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413 (last visited Aug. 1, 2024).

[274] Official Website of the EU, *Digital Services Act: Questions and Answers* (Apr. 3. 2024), https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers (last visited Aug. 1, 2024).

[275] Official Website of the EU, *The Digital Markets Act: Ensuring Fair and Open Digital Markets*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en (last visited Aug. 1, 2024).

[276] Article 52 of the 2021 PIPL.

[277] Article 11 of the 2013 Personal Information Provisions.

[278] Article 58 of the 2021 PIPL.

independent organization may overlap, which is similar to the functional overlapping of the board of supervisors and independent directors in listed companies.[279] The disorganization in corporate governance will make it difficult for data processors to comply with data protection laws.

VI. CONCLUSION

This Article conducted in-depth analyses of China's personal data protection regulatory system from doctrinal, comparative, and empirical perspectives. China's data protection laws have gone through several historical stages, with the focus gradually shifting from network infrastructure construction to cybersecurity and personal information protection. In recent years, China has enacted the 2016 Cybersecurity Law and the 2021 PIPL to enhance personal data protection, covering critical issues such as public interest protection and VLOP gatekeeper mechanism. To streamline the public enforcement of data protection laws, the regulatory institution structure at the state level has transitioned from the single regulator model (the MIIT) to the twin peaks model (the CAC and the MIIT). At the local level, local governmental agencies, notably public security bureaus, have helped the CAC in undertaking regulatory powers.

This Article analyzed fifty-one administrative penalty cases handled by the CAC and local security bureaus, as well as 1,233 app cases handled by the MIIT. After the PIPL was issued in 2021, the number of cases peaked. Though the CAC handled only two cases (DiDi and CNKI), it imposed huge fines. Local cases were concentrated in developed provinces such as Jiangsu and Guangdong. Small enterprises are major targets of penalties, while VLOPs were rarely sanctioned due to local protectionism. The main forms of penalties were warnings and orders to make corrections, reflecting the cautious attitude of regulators. The MIIT regularly publishes lists of apps that violate personal information rights, which is a deterrent for data processors. Most app developers are organizations located in Beijing, Guangdong, Shanghai, and Zhejiang, where the most developed private economy and internet enterprises are domiciled. App downloads are mainly from software app stores operated by VLOPs such as Tencent.

In the public enforcement of data protection laws, the EU, the U.S., and China have divergent institutional structures. Unlike the U.S. and the

[279] Donald C. Clarke, *The Independent Director in Chinese Corporate Governance*, 31 (1) DEL. J. OF CORP. L. 125 (2006).

EU, China has adopted a two-tier regulatory model. Under the twin peaks model at the state level, the CAC tends to invoke catch-all provisions, while the MIIT focuses on the specific activities of app developers such as collecting and using personal information illegally or excessively. This twin peaks model has certain advantages, such as monitoring data processors from both data processing and app development, achieving, and avoiding regulatory arbitrage. At the local level, China decentralized regulatory powers to local governmental agencies (public security bureaus of municipal and district/county levels), resulting in inconsistent enforcement standards. This Article argues that China should learn from the EU model under which the EU and its member states cooperate to solve inconsistencies in law enforcement.

The EU, the U.S., and China also have divergent administrative penalties. Since the 2021 PIPL was enacted, China's case numbers have been growing fast. Chinese regulators focus on illegal collection of personal information, while EU regulators attach great importance to applying basic principles. Compared with China and the U.S., the EU has much harsher monetary sanctions on data processors. China's exemption mechanism mainly protects the interests of government agencies, while the EU exemption rules focus on balancing the interests of users and platforms. These divergences are caused by different political and economic contexts. On one hand, American tech giants have great influence in Europe, so the EU attempts to curb foreign big tech firms to protect local platforms with hash regulation. On the other hand, China's national strategy is to foster digital platforms to fulfill the country's global ambitions. It is natural for the government to relieve domestic VLOPs of too much of a legal compliance burden to achieve global competitive advantages over American VLOPs in the Sino-U.S. tech war. Therefore, this Article predicts that China will not wholly adopt the stringent EU model in the future. Instead, China will converge with the U.S. by maintaining low monetary sanctions, thus achieving a balance between data protection regulatory goals and national development agendas. To this end, China should improve the exemption mechanism to prevent technology companies from taking excessive liability risks.

China's "public interests" are embodied in the ideological censorship and national security review conducted by data processors on users' information. It is concerning that the Chinese government might enlarge their control over the dissemination of information since it has a final say on what China's national interests and ideology standards are. The 2021 PIPL regulates automated decision-making in a forward-looking sense, but the rules are too general. China should learn from the EU's experience in tackling specific problems of automated decision-making. Although China has set up specific rules for VLOPs as gatekeepers, VLOPs were rarely sanctioned in practice. Chinese law needs to strike a balance between encouraging the development of VLOPs and protecting personal data. In addition, China should establish specific identification criteria for VLOPs and strengthen their supervision by designing new obligations for VLOPs. To supervise the gatekeepers, Chinese law has set up a "personal information protection officer" and independent external organization. It remains to be seen whether they can undertake the expected functions.