Università
Ca'Foscari
Venezia

Master's Degree programme

in Language and Management to China

Final Thesis

China's New Personal Information Protection Law (PIPL): Implications for Companies and Human Resources Management

Supervisor
Ch. Prof. Renzo Riccardo Cavalieri

Graduand
Rachele Torrisi
Matriculation Number 890721

Academic Year
2022/2023

前言

近年来，随着互联网的普及，数字经济正在成为经济的重要力量，并也成为了未来的重点发展方向之一。统计显示，截至 2021 年 6 月，中国网民规模达 10 亿，互联网普及率达 71.6%。十亿用户接入互联网，形成了全球最大的数字社会。根据统计，2020 年中国数字经济规模已达到 39.2 万亿元，占 GDP 比重达 38.6%。此外，新冠疫情使数字经济快速发展,因为，网上购物、在线教育、远程办公、智慧医疗进入了人们的日常生活 。

随着网民规模的变大 ，网络个人的信息量也越来越大 ，这些 个人信息包括姓名、住址、工作单位、身份证号，等等。其实，这种信息对企业非常重要，因为所有的企业都利用个人信息来改善运营，提供更好的客户服务，创建个性化的营销活动，并最终提高盈利能力。因此，如果企业有效地利用个人信息，他们就可以拥有竞争优势。

数字经济的发展虽然带来了许多好处，但是在它的应用过程中还存在很多问题。

首先，个人信息在规模化的商业利用中具有巨大的经济价值。不过，它们也造成了 信息主体、企业及国家之间的利益冲突。

其次，一些企业、机构或者个人为谋取商业利益 ，肆意收集、违法获取、过度使用、非法买卖个人信息。

最后，随着技术的进步，手机 APP 有能力获取并公开用户的个人信息，因此个人隐私无法得到足够的保障。

近年来，中国政府承认数据在推动国家现代化建设中的 基础性、战略性作用。此外，中国政府也将数据当作了国家的基础性战略资源。

同时，随着信息技术的不断发展，中国政府与公民都已经深刻认识到了技术运用可能会给个人与国家安全带来的风险。

因此，中国政府开始开始思考如何在保护个人隐私的前提下实现个人信息的合法与合理应用。结果是，中国政府意识到了据治理的重要性。

中国《个人信息保护法》明确个人信息处理一般规则及处理过程中的个人与信息处理者之间的权利义务关系。

2021 年 8 月 20 日《中华人民共和国个人信息保护法》由第十三届全国人民代表大会常务委员会第三十次会议审议通过并公布，并于 2021 年 11 月 1 日起施行。

《个人信息保护法》与《网络安全法》、以及《数据安全法》一起，成为中过网络空间管理和数据保护的“三驾马车”。

《个人信息保护法》共八章，总计七十四个条款。其中，第一章为“总则”。第二章为“个人信息处理规则”（包括第一节“一般规定”、第二节“敏感个人信息的处理规则”与第三节“国家机关处理个人信息的特别规定”)。第三章为“个人信息跨境提供的规则”。第四章为“个人在个人信息处理活动中的权利”。第五章为“个人信息处理者的义务”。第六章为“履行个人信息保护职责的部门”。第七章为“法律责任”。第八章为“附 则”.

因此，《个人信息保护法》明确个人信息处理一般规则及处理过程中的个人与信息处理者之间的权利义务关系。

本论文主要分析《个人信息保护法》及其对国内外公司造成的主要影响 ，包括其对这些公司相关业务活动造成的影响。

论文分为三章。

总体上，第一章分析该法的历史与立法背景，该法的关键点以及隐私和个人信息保护的区别。

首先， 《个人信息保护法》 是中国政府对数据保护日渐重视的证明 。对数据保护的日渐重视由以下四个因素推动。

第一、数字化的政府系统的出现。

第二、个数字经济 的发展与平台企业的崛起。总体来说，平台企业商业模式的基础就是用户数据的收集与使用。

第三、网上黑市的发展，在其中，大量的个人信息被买卖。

第四、信息化发展导致数据泄露与被攻击的可能性增大了。

个人信息保护法》的最终文本公布前，中国政府已公布了两本草案。因此，本文将会分析此三部文本之间的区别与关联。

此外， 第一章还会分析《个人信息保护法》的要点，包括该法的目的（即保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用）、个人信息与个人信息处理者的含义与个人信息的内涵与匿名化。

在第一章的结尾将会解释在中国“隐私”与“个人信息”的不同含义。为了理解中国《个人信息保护法》与中国客户的文化，所有企业都应该明白它们的区别。

第二章分析该法对公司造成的影响 ，其中包括企业的义务，违反该法时的责任，以及对两个主要业务领域的影响：数字营销和数字广告。

首先，关于企业的义务，本文分析《个人信息保护法》第五章。根据第51条，为了避免个人信息泄露、篡改及丢失，所有个人信息处理者都应该采取一些措施，比如说：定期对从业人员进行安全教育和培训或者制定并组织实施个人信息安全事件应急预案。

此外，根据第54条，个人信息处理者也应该进行合规审计 。并且，根据第55条，在五种情况下，他们应该进行个人信息保护影响评估。这些情况包括：敏感个人信息的处理、个人信息进行自动化决策的利用、个人信息的向境外提供，等等。第56条解释该个人信息保护影响评估的内容。

其次，根据《个人信息保护法》第 5 至 9 条，处理人们个人信息时，个人信息处理者应该遵守七个原则，包括合法、必要和诚信原则，透明原则等等。

再次，《个人信息保护法》第七章解释法律责任。如果处理个人信息者未履行该法规定的个人信息保护义务，他们就会面临严重后果。比如说，由履行个人信息保护职责的部门责令改正或者给予警告。本文第二章将 提供滴滴出行公司的案例来解释法律责任。

最后，中国《个人信息保护法》对企业造成的影响不仅包括企业义务或者法律责任，还包括 包括该法对数字营销与数字广告的影响。其实，为了履行《个人信息保护法》，企业应该减少他们处理的用户个人信息数量。因此，他们需要改变其商业模式。

第三章分析人力资源管理与雇主和雇员的关系。

首先，本章分析雇主怎么收集、处理及转移雇员的个人信息。根据《个人信息保护法》第 13 条，在实施人力资源管理的情况下，雇主不需要雇员的同意来处理其个人信息。不过，总体上，为了处理雇员的个人信息，有三个处理个人信息的合法性基础：人们同意、履行一个合同所必需，或者实施人力资源管理所必需。

其次，本章分析个人信息的境外提供。该方面在《个人信息保护法》第三章进行了解释 。根据该法第 38 条，如果企业将中国人个人信息转移到中国境外，他们应该采取三个措施。第一、通过国家网信部门组织的安全评估；第二、经专业机构进行个人信息保护认证；第三、与境外接收方订立合同。本章将深入分析这三个措施 。

最后，处理雇员的个人信息时，有时人信息保护者不遵守上述原则。比如说，雇主常常过度收集雇员个人信息及敏感个人信息。此外，存在

未经雇员同意，雇主私自收集并处理其个人信息的情况。本章将提供一些案件来解释《个人信息保护法》的实施。

总结全文，不管是中国还是境外企业，中国《个人信息保护法》对所有企业都造成了巨大的影响。《个人信息保护法》的实施使所有企业都改变了他们的商业模式，以及他们处理用户或者雇员个人信息的办法。

Table of contents

Introduction

As Dev Lewis – sinologist and fellow and program Lead at Digital Asia – states, the global economy is undergoing a transformation widely recognized as the fourth industrial revolution made possible by data driven intelligent systems.[1] As a consequence, policy makers around the world are developing new regulatory frameworks in order to help societies manage the potential risks these new systems bring to society.[2]

With a specific focus on China, Chinese policy makers are attaching great attention to the construction of legal regimes, in order to govern data from two points of view: national security and economic development.

There are three main laws which regulate data processing activities in China: The Cybersecurity Law, the Data Security Law and the Personal Information Protection Law.

This thesis mainly focuses on the analysis of the Personal Information Protection Law (PIPL) and its main impacts on domestic and foreign companies, together with the impacts on their relevant business activities.

Chapter I of this thesis mainly analyzes the historical and regulatory background of the Law; the key points of the Law; and the difference between the concepts of privacy and personal information.

Chapter II analyzes the Law's implications on companies, that include companies' obligations, liabilities in case of violation of the Law, as well as the impacts on two main business areas: digital marketing and digital advertising.

Chapter III analyzes human resources management, with a focus on the methods to collect, process, and transfer of employees' personal data. This chapter ends with an analysis of different judicial cases which show how the processing of personal information can affect the employment relationship between employer and employee.

[1] Lewis, Dev, *Data Sovereignty in Action: Ant Group and Didi Chuxing Case Studies*, Digital Asia Hub, 12/09/2022. Available at: https://www.digitalasiahub.org/2022/09/12/data-sovereignty-in-action-ant-group-and-didi-chuxing-case-studies/?utm_source=rss&utm_medium=rss&utm_campaign=data-sovereignty-in-action-ant-group-and-didi-chuxing-case-studies (Last Access: 01/06/2023)
[2] Ibid.

Chapter 1. China Personal Information Protection Law (PIPL)

Since the arrival of consumer internet in the 1990s, the collection of individuals' data has increased exponentially and have not slowed down over the last decades.[3]

The Internet is now an essential component of everyone's daily life, and has profoundly changed the way individuals work, conduct their personal lives, and interact with other people. One consequence of this development is that individuals' routine online activities, such as email, search, and online shopping, constantly generate data about them.[4]

For a long time, companies have collected consumers' data unabated, and consumers did not express their concerns[5]. However, given the greater integration of technology in every aspect of private and public life, the situation started to change.

In fact, the massive and unprecedented scale of personal data generation in conjunction with rapid reductions in computing costs for data storage and analytics have led to serious privacy concerns by the public and policy makers.[6]

Consumers have become more concerned about how their personal data is collected and are facing the simultaneous need to maintain privacy and reveal personal information for the purpose of obtaining diverse services.[7]

Among the reasons that have led to an increase of privacy concerns, the major one is that consumers started to be aware of the quantity of their personal information that was collected and used by companies.

For what concerns China, in recent years, with the rapid development of Internet of things (IoT) and online shopping with mobile payments, consumers offer their personal information to purchase items on online platforms (e.g., Taobao 淘宝 or JD.com 京东), as a result of the ability to shop 24/7 and the trust that exists between buyers and sellers.

---

[3] Goswami, Swish, The Rising Concern Around Consumer Data and Privacy, Forbes, 14/12/2020. Available at: https://www.forbes.com/sites/forbestechcouncil/2020/12/14/the-rising-concern-around-consumer-data-and-privacy/

[4] Jay, Pil Choi, Doh-Shin, Jeon, Byung-Cheol, Kim, *Privacy and personal data collection with information externalities*, Journal of Public Economics, Volume 173, 2019, pp. 113-124, https://doi.org/10.1016/j.jpubeco.2019.02.001

[5] Goswami, Swish, The Rising Concern Around Consumer Data and Privacy, Forbes, 14/12/2020. Available at: https://www.forbes.com/sites/forbestechcouncil/2020/12/14/the-rising-concern-around-consumer-data-and-privacy/

[6] Jay, Pil Choi, Doh-Shin, Jeon, Byung-Cheol, Kim, *Privacy and personal data collection with information externalities*, Journal of Public Economics, Volume 173, 2019, pp. 113-124, https://doi.org/10.1016/j.jpubeco.2019.02.001

[7] Calzada, Igor*, Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)*. Smart Cities 2022, 5, 1129–1150. https://doi.org/ 10.3390/smartcities5030057

However, such trust should not be underestimated by companies, which must focus on guaranteeing a greater information protection to consumers, in order to build a positive customer relation based on trust.

Not only consumers have become and are becoming more and more aware of their data rights and of how their data is used, but also governments have started to attach importance to such matter and have started to regulate data collection.

The reason of such concern is that, under the conditions of the digital economy, data privacy has become a global concern, and probably a geopolitical battleground in terms of data and digital sovereignty.[8]

In general, although there is the potential to derive enormous value from data, there is also a fundamental requirement to secure data, meaning both government and business must protect citizens' and consumers' personal information.[9]

Data governance can be defined as the way in which data is controlled, managed and optimized[10], and as the key to achieving the benefits of data optimization and mitigating the inherent risks, as it enables organizations to control data by securing, protecting, managing and optimizing the value of data.[11]

There are three major regulations on data governance: the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and China's Personal Information Protection Law (PIPL).

The Personal Information Protection Law (*Gerenxinxi Baohu Fa* 个人信息保护法[12]) was adopted at the 30th Session of the Standing Committee of the 13th National People's Congress of the PRC on August 20, 2021 and went into effect on November 1, 2021.

[8] Calzada, Igor, *Data Co-operatives through Data Sovereignty*. Smart Cities 2021, 4, 1158–1172. Special Issue "Feature Papers for Smart Cities".
[9] Bennett, Susan, *Risk Management: Data as a Strategic National Resource - the Importance of Governance and Data Protection*., Governance Directions 71.7 (2019): 362-66.
[10] Ibid.
[11] Ibid.
[12] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

Together with the Cybersecurity Law (*Wangluo Anquan Fa* 网络安全法[13]) and the Data Security Law (*Shuju Anquan Fa* 数据安全法[14]) of the PRC, the PIPL builds up a comprehensive and systematic legal framework for regulating data protection and cybersecurity.

Before moving to the analysis of the main contents of the PIPL, the Law's historical and regulatory context is worth an investigation.

1.1 Historical and regulatory context of the PIPL

As it was said at the beginning of this chapter, the rapid expansion of digital services, together with the increase in data generation, collection, processing, and use, have pushed data protection questions high on the political agenda in countries around the world[15].

Until the end of the 2000s, China had no dedicated data protection rules; however, since then, the situation changed, as great attention was attached by Chinese government to data protection, and such effort culminated in the promulgation of the Personal Information Protection Law and the Data Security Law in 2021.

The development of Chinese data protection regulation has reflected the evolving concerns and perception of the Chinese government towards the rapid introduction of digital technologies in China's state, economy, and society, and the potential impact of different forms of data abuse.[16]

This process of growing concern and attention towards data protection was driven by different factors.

[13] Zhonghua Renmin Gongheguo Hulianwang Xinxi Bangongshi 中华人民共和国国家互联网信息办公室 (The Cyberspace Administration of China), Zhonghua Renmin Gongheguo Wangluo Anquan Fa 中华人民共和国网络安全法 (The Cybersecurity Law of the PRC), 07/11/2016. Available at: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

[14] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), Zhonghua Renmin Gongheguo Shuju Anquan Fa 中华人民共和国数据安全法 (The Data Security Law of the PRC), 10/06/2021. Available at: http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml

[15] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p.1. Available at: https://doi.org/10.1093/cybsec/tyac011

[16] Ibid., p.2.

First, the emergence of digitized government systems[17], which started with the "Golden Projects[18]" of the 1990s and continued at present with a new Five-Year Plan for Governmental Informatization[19]. These projects required that the government authorities could obtain the data they needed – including personal information – to make China more efficient and effective at fulfilling its tasks, such as in public services or the maintenance of social stability.[20]

The second factor was the development of digital economy with the rise of large platform companies, which based their business model on the exploitation of user data.

The third factor was the rise of a large black market in which personal information was traded by corporate and governmental insiders as a consequence of the increasing economic value of data.

The fourth factor was the increase of data-related leaks, hacks and attacks, due to the progress of informatization.

Although the legislative responses to the above-mentioned aspects were slow, the Party leadership attached great attention to securing network information[21].

The first attempt to secure network information was made in 1994, when the Ministry of Public Security (MPS) developed a tiered approach that would impose differing levels of requirement based on the importance of specific network systems[22]: a multi-level protection system (*Xinxi Anquan Dengji Baohu Zhidu* 信息安全等级保护制度[23]).

---

[17] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p.2. Available at: https://doi.org/10.1093/cybsec/tyac011

[18] The Golden Projects refer to the Chinese government's systematic acceleration of IT infrastructure deployment in state agencies, schools, and hospitals. The three major Golden Projects were Golden Card, Golden Customs and Golden Tax, which began in 1990. (https://mic.iii.org.tw/English/reports_detail.aspx?DataClass=Communications&sqno=1412&SubDataClass=Mobile%20Handheld%20Devices&type=&SubSqno=18#:~:text=The%20Golden%20Projects%20refer%20to,Golden%20Tax%20%2D%20began%20in%201990)

[19] Zhonghua Renmin Gongheguo Zhongyang Renmin Zhengfu 中华人民共和国中央人民政府 (Central People's Government of the People's Republic of China), Guojia Fazhan Gaige Wei Guanyu Yinfa "Shisiwu Tuijin Guojia Zhengwu Xinxihua Guihua" de Tongzhi 国家发展改革委关于印发《"十四五"推进国家政务信息化规划》的通知 (Notice of the National Development and Reform Commission on Printing and Distributing the "14th Five-Year Plan for Promoting National Government Informationization"), 2021. Available at: http://www.gov.cn/zhengce/zhengceku/2022-01/06/content_5666746.htm

[20] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p.2. Available at: https://doi.org/10.1093/cybsec/tyac011

[21] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p.3. Available at: https://doi.org/10.1093/cybsec/tyac011

[22] Ibid.

[23] To know more, please read: Beijing Huagong Daxue 北京化工大学 (Beijing University of Chemical Technology), Guanyu Xinxi Anquan Dengji Baohugongzuo De Shishi Yijian 关于信息安全等级保护工作的实施意见 (Implementation Opinions concerning the Information Security Multi-Level Protection System), 14/09/2012. Available at: https://cit.buct.edu.cn/2012/0914/c7951a95007/page.htm

This multi-level protection system (MLPS) was finalized in 2007, and aimed to raise information security protection capabilities and levels, safeguard national security, social stability and the public interest, safeguard and stimulate the healthy development of informatization construction[24].

It contained five security protection tiers: the self-protection tier (*zizhu baohu ji* 自主保护级), the guided protection tier (*zhidao baohu ji* 指导保护级), the supervised protection tier (*jiandu baohu ji* 监督保护级), the mandatory protection tier (*qiangzhi baohu ji* 强制保护级), and the specially controlled protection tier (zhuan kong baohu ji 专控保护级).[25]

These tiers went from the one dealing with information systems which did not harm national security, public interest, economic construction or social order, to the ones – the fourth and the fifth – applied to those information systems whose destruction could result in grave and especially grave harm to national security, social order, economic construction and the public interest.[26]

Therefore, this system constructed an institutional and conceptual framework for the protection of digital assets from the perspective of national security, the lifelines of the economy and social stability.[27]

Although the MLPS did not protect data *per se* – as it rather constituted a protection regime for all network systems that protected them in their entirety – this protection system laid the groundwork for the introduction of the DSL regime[28].

A second attempt occurred when the State Council Informatization Office commissioned Zhou Hanhua 周汉华– who is now vice president of the Institute of Law at the Chinese Academy of Social Sciences – to lead the drafting of a legislative proposal for personal information protection, which was published in 2006.

---

[24] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p.3. Available at: https://doi.org/10.1093/cybsec/tyac011

[25] Creemers, Rogier, *Implementation Opinions concerning the Information Security Multi-Level Protection System*, China Copyright and Media, The Law and policy media in China, 14/09/2012. Available at: https://chinacopyrightandmedia.wordpress.com/2004/09/15/implementation-opinions-concerning-the-information-security-multi-level-protection-system/ (Last access 18/05/2023)

[26] Creemers, Rogier, *Implementation Opinions concerning the Information Security Multi-Level Protection System*, China Copyright and Media, The Law and policy media in China, 14/09/2012. Available at: https://chinacopyrightandmedia.wordpress.com/2004/09/15/implementation-opinions-concerning-the-information-security-multi-level-protection-system/ (Last access 18/05/2023)

[27] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p.3. Available at: https://doi.org/10.1093/cybsec/tyac011

[28] Ibid.

This "Expert Suggestion Draft" (*zhuanjia jianyi gao* 专家建议稿) laid down ten principles for data protection, and addressed data collection and processing by government bodies. The draft is one of the outcomes of the National Social Science Fund Major Project "Important Legislative Questions for Internet Security" (14ZDC021) at Renmin University of China Law School, of which Professor Zhang Xinbao is lead expert, and its objective is to provide reference for legislation.[29]

Furthermore, the draft is based on the theoretical idea of "strengthening two pillars, balancing three sides", which means that, by strengthening the protection of sensitive personal information and strengthening the use of ordinary personal information, it realizes balance between the interest of subjects on three sides: information subjects, information businesses and state bodies.[30]

The Expert Suggestion Draft was characterized by different elements.

First, it contained fairly strict limitations on data collection as well as a requirement to register collection processes with a relevant agency in charge, although wide exceptions were included for areas such as security and policing[31].

Second, it addressed data collection by "other data processors" in the private sector, requiring them to register with an appropriate authority.[32]

Third, it included restrictions on cross-border transfer of personal information, but only for private sector actors.[33]

Fourth, in terms of enforcement, it did not refer to a dedicated data regulator, but to a mix of complex administrative enforcement and judicial enforcement processes[34].

However, Zhou's Expert Suggestion Draft was never adopted as formal legislation.

Two other regulatory efforts occurred in 2011.

The first one occurred when the People's Bank of China (*zhongguo renmin yinhang* 中国人民银行) released a circular on protecting individuals' banking and financial information.

---

[29] Creemers, Rogier, *Personal Information Protection Law (Expert Suggestion Draft*), DigiChina, Stanford University, 17/10/2019. Available at: https://digichina.stanford.edu/work/personal-information-protection-law-expert-suggestion-draft/ (Last access 18/05/2023)
[30] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p.3. Available at: https://doi.org/10.1093/cybsec/tyac011
[31] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p.3. Available at: https://doi.org/10.1093/cybsec/tyac011
[32] Ibid.
[33] Ibid.
[34] Ibid.

As Rogier Creemer argues, this document can be considered the first instance of mandatory data localization, as it required that personal information which was collected in China must be stored within the borders of the PRC and strictly regulated outbound conditions[35].

The second effort was constituted by the Regulations for Internet information services[36] released by the Ministry of Industry and Information Technology (MIIT).

These regulations established the principles of informed consent, and necessity for data collection and use; created obligations to notify authority in case of serious data breaches; gave users the rights to revise and delete their personal information, and prohibited online service providers from transferring or trading personal information.[37]

Although the above-mentioned aspects made the regulations extremely innovative, the regulations' enforcement strength was limited, as the highest punishment that could be imposed was a fine of 30 000 RMB.[38]

Nevertheless, the MIIT's regulations constitute a crucial event in the process of data protection regulation, as they demonstrate that the online economy had gained priority in personal information protection.

In 2013, the MIIT supplemented these regulations with a technical standard[39], which, for the first time, contained clear terminological definitions and basic norms.

Although this document was not legally binding, it carried considerable normative authority.[40]

---

[35] Liu, Jinhe, *China's data localization*, Chinese Journal of Communication, 13, 1-20, 2019. https://doi.org/10.1080/17544750.2019.1649289

[36] Zhonghua Renmin Gongheguo Zhongyang Renmin Zhengfu 中华人民共和国中央人民政府 (Central People's Government of the People's Republic of China), Guifan Hulianwang Xinxi Fuwu Shichang Zhixu Ruogan Guiding 规范互联网信息服务市场秩序若干规定 (Some Provisions to Standardize Internet Information Service Market Order), 29/12/2011. Available at: http://www.gov.cn/gongbao/content/2012/content_2161726.htm

[37] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p.3. Available at: https://doi.org/10.1093/cybsec/tyac011

[38] Zhonghua Renmin Gongheguo Zhongyang Renmin Zhengfu 中华人民共和国中央人民政府 (Central People's Government of the People's Republic of China), Guifan Hulianwang Xinxi Fuwu Shichang Zhixu Ruogan Guiding 规范互联网信息服务市场秩序若干规定 (Some Provisions to Standardize Internet Information Service Market Order), 29/12/2011. Available at: http://www.gov.cn/gongbao/content/2012/content_2161726.htm

[39] Xinxi Anquan Jishu Gonggong Ji Shangyong Fuwu Xinxi Xitong Geren Xinxi Baohu Zhinan 信息安全技术公共及商用服务信息系统·个人信息保护指南 (Information Security Technology Guidelines for Personal Information Protection on Public and Commercial Service Information Systems), 21/01/2013. Available at: https://digichina.stanford.edu/work/information-security-technology-guidelines-for-personal-information-protection-on-public-and-commercial-service-information-systems/

[40] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p.3. Available at: https://doi.org/10.1093/cybsec/tyac011

From 2012 onward, the Chinese government have tried to centralize data governance, and create more generalized legislative frameworks, moving away from sector-specific interventions.[41]

An example of such centralization on data regulation was the establishment of the Cyberspace Administration of China (CAC) *guojia hulianwang xinxi bangongshi* 国家互联网信息办公室, which is in charge of cyberspace security and internet content regulation.[42]

The establishment of the CAC is extremely important, as before its establishment, China's Internet institution was decentralized according to the so-called "water harnessing by nine dragons" (*jiulong zhishui* 九龙治水) model, which means that the Chinese Internet was managed by more than 10 ministries and departments with unclear responsibilities.[43]

The period which extends from 2012 to nowadays is characterized by two aspects.

First, a huge support by the Chinese government to the new business landscape characterized by big Internet platforms – e.g., Alibaba, Tencent, Bytedance – whose business model was based on the collection and analysis of users' data. In fact, in 2015, the Chinese government issued an action plan on big data, which defined data as a basic strategic resource.[44]

Second, the rise of a black market characterized by a great abuse of individuals' personal data. Actually, that period was characterized by numerous cases of illegal sales of users' personal information by corporate employees and contractors, as well as government officials and departments.[45]

This is the reason why in the period between 2012 and 2016 the main developments were focused on consumer protection.

Evidences of a greater concern towards consumer protection are the Decision on Information Protection (*jiaqiang wangluo xinxi baohu de jueding* 加强网络信息保护的决

[41] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p.3. Available at: https://doi.org/10.1093/cybsec/tyac011
[42] Cyberspace Administration of China (CAC), Glossary, Reuters. https://uk.practicallaw.thomsonreuters.com/8-618-2325?transitionType=Default&contextData=(sc.Default)&firstPage=true
[43] Liu, Jinhe, *China's data localization*, Chinese Journal of Communication, 13, 1-20, 2019. https://doi.org/10.1080/17544750.2019.1649289
[44] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p.3. Available at: https://doi.org/10.1093/cybsec/tyac011
[45] Ibid., p. 4.

定[46]) issued by the National People's Congress Standing Committee in 2012. Not only it created an obligation for online businesses to delete published personal information, or address related infringement in other appropriate ways, but also addressed data use in government departments, prohibiting them from leaking, distorting, or selling personal information.[47]

The Decision coincided with a strengthening of enforcement efforts: in fact, in early 2013, the Supreme People's Court, Supreme People's Procuratorate and MPS issued a notification that pushed police, prosecutorial, and judicial bodies to tackle personal data infringement more strictly, through the application of criminal prosecution.[48]

In addition, this period in China was characterized by a huge attention attached to data securitization and the control of online data. In fact, the worsening relationship between China and US, as well as the growing concern about terrorism, made the Chinese government realize that the lines between protecting personal information for the sake of the individual interest, and its potential relevance for national security, had started

to blur.[49]

As a consequence, new data localization requirements were imposed in

fields extending from the credit, mapping, and healthcare sectors to online publishing and cloud service.[50]

These concerns led to the drafting of the Cybersecurity Law (CSL), which contained a section on personal information protection and a first mention of the term "important data" (*zhongyaoshuju* 重要数据).[51]

[46] Zhonghua Renmin Gongheguo Zhongyang Renmin Zhengfu (Central People's Government of the People's Republic of China 中华人民共和国中央人民政府, Quanguo Renda Changwei Hui Guanyu Jiaqiang Wangluo Xinxi Baohu De Jueding 全国人大常委会关于加强网络信息保护的决定 (National People's Congress Standing Committee Decision concerning Strengthening Network Information Protection), 28/12/2012. Available at: http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm

[47] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p. 4. Available at: https://doi.org/10.1093/cybsec/tyac011

[48] Ibid.

[49] Ibid.

[50] Liu, Jinhe, *China's data localization*, Chinese Journal of Communication, 13, 1-20, 2019. https://doi.org/10.1080/17544750.2019.1649289

[51] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p. 4. Available at: https://doi.org/10.1093/cybsec/tyac011

However, the implementation of the CSL met different obstacles, among which the big tech giants' opposition to the introduction of a stricter privacy law, and bureaucratic issues, as the Ministry of Public Security loath to transfer its data-related competences to the CAC.[52]

The CSL finally came into effect in 2017, and constitutes the cornerstone of

a new and comprehensive regime that seeks to secure the Chinese digital sphere and integrate cybersecurity-related policy areas and the bureaucratic actors involved.[53]

As China's first basic Internet law governing cybersecurity, the Cybersecurity Law contains several major principles and innovations, such as cyberspace sovereignty, a hierarchical system for cybersecurity protection, a critical information infrastructure protection system, a security assessment system for cross-border data transfers, and a security review system for network products and services.[54]

Moreover, the CSL is characterized by two main elements: the incorporation of the substantive provisions from the 2012 Decision; and the introduction of the concept of "important data," even if it did not provide a detailed definition.

The CSL also led to a strengthening of enforcement, as non-compliance with personal information protection requirements could lead to punishment ranging from a simple warning to fines of up to 1 million RMB, suspension or closure of websites, or cancellation of related business licenses.[55]

Lastly, the Cybersecurity Law defines Personal information as:

> various information recorded in electronic or other means that can lead to the identification of a natural person, including but not limited to the natural person's name, date of birth, identity card number, personal biometric information, address, telephone number and so on.[56]

---

[52] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p. 4. Available at: https://doi.org/10.1093/cybsec/tyac011

[53] Ibid.

[54] Aimin Qi, Guosong Shao, Wentong Zheng, *Assessing China's Cybersecurity Law*, Computer Law & Security Review, Volume 34, Issue 6, 2018, p. 1342-1354, ISSN 0267-3649. https://doi.org/10.1016/j.clsr.2018.08.007

[55] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p. 4. Available at: https://doi.org/10.1093/cybsec/tyac011

[56] Zhonghua Renmin Gongheguo Zhongyang Renmin Zhengfu 中华人民共和国中央人民政府 (Central People's Government of the People's Republic of China), Zhonghua Renmin Gongheguo Wangluo Anquanfa 中华人民共和国网络安全法 (The Cybersecurity Law of the PRC), 07/11/2016. Available at: http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm

Although the emanation of the CSL was extremely important, the new Law left different questions unanswered[57], such as the ones related to the cross-border data transfer and, in general, to data protection. In fact, according to Hong Yanqing, the Law did not provide systemic thinking, let alone comprehensive institutional designs[58], to effectively protect the data.[59]

Moreover, the CSL increased the tensions between the CAC and the MPS, as it did not specify which departments would take charge of implementing the Law.

After the CSL went into effect, the two authorities – the CAC and the MPS issued several data-related mandates, which, however, never passed or took effect.

Given the continuous growth of the perceived importance of data in economic, social and governmental process, in 2020 the Central Committee officially defined data as an essential factor of production, equal to land, capital and labor.[60]

At the same time, there also was an increasing demand for a more effective data-related regulation, in particular with regard to the big tech giants' business models based on the collection of data.

In order to respond to such matter, in 2019 the CAC, MIIT, MPS, and the State Administration of Market Regulation (SAMR) jointly supervised the creation

of an "App Governance Working Group" (*App zhuanxiang zhili gongzuozu* App 专项治理工作组), comprising TC260[61] and several industry associations[62], which released various standards and regulations on information collection and use in mobile apps.

Simultaneously, a rising motivation to adopt a more integrated approach towards the digital economy aimed at shaping online business models led to the drafts of the PIPL and the DSL, which came into effect on November 1, 2021 and September 1, 2021 respectively.

---

[57] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p. 4. Available at: https://doi.org/10.1093/cybsec/tyac011

[58] Hong Yanqing 洪延青, *Wangluo Anquan Fa Dui Shuju Anquan Baohu Zhi De Yu Shi*《网络安全法》对数据安全保护之得与失 *(On the Gain and Loss of Cybersecurity Law of China on Data Protection*). Zhengce Pinglun 政策评论 (Pol Rev) 2017;1: 66–73. http://library.ttcdw.com/uploadfiles/zk/1507792951.pdf

[59] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p. 4. Available at: https://doi.org/10.1093/cybsec/tyac011

[60] Ibid., p. 5.

[61] The National Information Security Standardization Technical Committee of China, also known as TC260.

[62] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p. 5. Available at: https://doi.org/10.1093/cybsec/tyac011

The Data Security Law covers all data except for state secrets, and it mainly focuses on national security and the public interest.

If compared with the PIPL, which aims to provide actionable provisions for businesses, the DSL is more programmatic, calling for the establishment of a strategy involving the "intelligentization[63]" of public services, research into data development and technology, the formulation of data-related standards, the promotion of a cybersecurity industry, the

establishment of data trading markets, and data-related education.[64]

1.2. Evolution of the Law: the first draft, the second draft and the final text of the PIPL

As it can be noticed by the events analyzed in the previous paragraph, the road that led to the final text of the PIPL was long, complex and full of obstacles.

China's Personal Information Protection Law has a history which extends for more than fifteen years, and the final text – which came into effect on November 1, 2021– was preceded by two drafts, published in October 2020 and April 2021, respectively.

According to Zhou Hanhua – who was a protagonist in the process of development of the Law – there are two main reasons that it took such a long time before the official draft of the PIPL was released.

First, during China's government restructuring in 2008, the informatization task was handed over from the State Council Informatization Office to a bureau under the Ministry of Information Technology, resulting in less impetus compared to before.[65]

Second, the imperative for personal information legislation is closely linked to the development of information technology.

[63] A term which emerged in China to refer to the use of artificial intelligence with the decision-making capability. (https://www.igi-global.com/dictionary/intelligentization/117144)
[64] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p. 7. Available at: https://doi.org/10.1093/cybsec/tyac011
[65] Huang, Yehan, Shi, Mingli, *Top Scholar Zhou Hanhua Illuminates 15+ Years of History Behind China's Personal Information Protection Law*, DigiChina, Stanford University, 8/06/2012. Available at: https://digichina.stanford.edu/work/top-scholar-zhou-hanhua-illuminates-15-years-of-history-behind-chinas-personal-information-protection-law/ (Last Access 15/05/2023)

Before 2010, technologies like cloud computing, big data, and the Internet of Things had just emerged, not yet leading to as many personal information issues as today, when these technologies have penetrated people's daily lives, causing significant privacy intrusions.[66]

An analysis of the first and second draft of the PIPL and a comparison between them and the final text, is useful to understand the key aspects of the Law and, therefore, provides a clearer picture of the regulation.

The main differences between the drafts and the final law can be seen in the following matters: automated decision-making, legal basis for processing personal information, minors' personal information, cross-border data transfers, data portability, government handling of personal information, post-mortem data rights, and different obligations for large and small data handlers.[67]

First of all, regarding automated decision-making, the main difference between the first draft and the second one is that the first draft does not state that personal information handlers must provide a way for individuals to reject business marketing and information push carried out through automated decision-making.[68]

In addition, when dealing with automated decision-making, the second draft of the PIPL required transparency, fairness, and justice in decisions, as well as explanation of the process in case of a significant impact on individuals' rights and interests.

Moreover, the second draft also included the individuals' ability to opt out of algorithmic targeting or automated decision-making.[69]

The final text of the PIPL adds further requirements, as Article 24 of the Law prohibits personal information processors to engage in unreasonable differential treatment of

[66] Huang, Yehan, Shi, Mingli, *Top Scholar Zhou Hanhua Illuminates 15+ Years of History Behind China's Personal Information Protection Law*, DigiChina, Stanford University, 8/06/2012. Available at: https://digichina.stanford.edu/work/top-scholar-zhou-hanhua-illuminates-15-years-of-history-behind-chinas-personal-information-protection-law/ (Last Access 15/05/2023)

[67] Lee, Alexa, Shi, Mingli, Chen, Qiheng, Horsley, Jamie P., Schaefer, Kendra, Creemers, Rogier, Webster, Graham, *Seven Major Changes in China's Finalized Personal Information Protection Law*, DigiChina, Stanford University, 15/09/2021. Available at: https://digichina.stanford.edu/work/seven-major-changes-in-chinas-finalized-personal-information-protection-law/ (Last Access 16/05/2023)

[68] China Briefing Team, *China's Personal Information Protection Law: A Comparison of the First Draft, the Second Draft, and the Final Document*, China Briefing, 24/08/2021. Available at: https://www.china-briefing.com/news/chinas-personal-information-protection-law-a-comparison-of-the-first-draft-the-second-draft-and-the-final-document/ (Last Access 16/05/2023)

[69] Lee, Alexa, Shi, Mingli, Chen, Qiheng, Horsley, Jamie P., Schaefer, Kendra, Creemers, Rogier, Webster, Graham, *Seven Major Changes in China's Finalized Personal Information Protection Law*, DigiChina, Stanford University, 15/09/2021. Available at: https://digichina.stanford.edu/work/seven-major-changes-in-chinas-finalized-personal-information-protection-law/ (Last Access 16/05/2023)

individuals in trading conditions[70] and prohibits price discrimination through automated decision-making.[71] Moreover, Article 24 of the final text of the PIPL also requires that personal information handlers shall provide a convenient method to refuse automated decision-making methods (*bianjie de jujue fangshi* 便捷的拒绝方式[72]).

The last difference between the final text and the two drafts on this matter can be seen in the definition of automatic decision-making provided by Article 73.

In fact, the definition provided by the first and second draft is the following:

> An automatic decision-making refers to an activity in which personal information is used to automatically analyze and evaluate a person's behavior habits, hobbies or economic, health or credit status through computer programs and make decisions.[73]

By contrast, the definition provided by Article 73 of the final text of the PIPL removes the words "personal information is used to" and replaces them with "automatically analyzes".

Regarding the legal basis of processing personal information, the main difference between the second draft and Article 13 of the final text is that the latter expands the list of the lawful bases, as it adds the clause of contractual necessity, that is the necessity for the conclusion or performance of a contract.[74] This additional clause is extremely relevant, as it will have a huge impact in the employment context.

For what concerns the treatment of minors under 14's personal information, Article 15 of the first and second draft indicate that, in order to process personal information of minors under the age of 14, their parents or other guardians' consent is necessary.

---

[70] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[71] Lee, Alexa, Shi, Mingli, Chen, Qiheng, Horsley, Jamie P., Schaefer, Kendra, Creemers, Rogier, Webster, Graham, *Seven Major Changes in China's Finalized Personal Information Protection Law*, DigiChina, Stanford University, 15/09/2021. Available at: https://digichina.stanford.edu/work/seven-major-changes-in-chinas-finalized-personal-information-protection-law/ (Last Access 16/05/2023)

[72] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[73] China Briefing Team, *China's Personal Information Protection Law: A Comparison of the First Draft, the Second Draft, and the Final Document*, China Briefing, 24/08/2021. Available at: https://www.china-briefing.com/news/chinas-personal-information-protection-law-a-comparison-of-the-first-draft-the-second-draft-and-the-final-document/ (Last Access 16/05/2023)

[74] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

However, there are different changes in the final text of the PIPL: first, the article which refers to minors under the age of 14 is Article 31; second, the final Law defines minors' personal data as sensitive personal information[75]; third, Article 31 of the PIPL adds that personal information handlers must formulate specialized rules for processing the personal information of minors under the age of 14.[76]

When making a comparison between the two drafts and the final text, it is also necessary to focus on cross-border data requirements.

The main difference between the first and the second draft is that the former provided the three conditions under which personal information can be transferred abroad, while the latter also adds that the contract with the overseas recipient must be in accordance with the standard contract formulated by the Cyberspace Administration of China (CAC)[77].

In addition, a further difference can be noticed in Article 43 replaces *corresponding* (*xiangying* 相应) with *reciprocal* (*duideng* 对等) which embodies the basic principles of international law and clarifies the limits of China's relevant countermeasures.[78]

What emerges from such comparison is that the final text of the PIPL provides a more detailed framework, and it includes a new provision explicitly allowing cross-border transfer of personal information when treaties or international agreements are in place.[79]

At the same time, the final text also imposes a new requirement on personal information exporters to ensure data protection standards are met after transfer.[80]

---

[75] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[76] Ibid.

[77] China Briefing Team, *China's Personal Information Protection Law: A Comparison of the First Draft, the Second Draft, and the Final Document*, China Briefing, 24/08/2021. Available at: https://www.china-briefing.com/news/chinas-personal-information-protection-law-a-comparison-of-the-first-draft-the-second-draft-and-the-final-document/ (Last Access 16/05/2023)

[78] *Cong Gerenxinxi Baohufa Ancao Ershengao Bianhua Kan Lifaqushi Ji Hegui Yaodian* 从个人信息保护法草案二审稿变化看立法趋势及合规要点 (*Legislative trends and compliance points from the changes in the second draft of the Personal Information Protection Law*), Simmons&Simmons, 08/05/2021. Available at: https://www.simmons-simmons.com/en/publications/cktbiji8f1zsm0a42cpz5heqb/simmons-data-observation-4 (Last Access 18/05/2023).

[79] Lee, Alexa, Shi, Mingli, Chen, Qiheng, Horsley, Jamie P., Schaefer, Kendra, Creemers, Rogier, Webster, Graham, *Seven Major Changes in China's Finalized Personal Information Protection Law*, DigiChina, Stanford University, 15/09/2021. Available at: https://digichina.stanford.edu/work/seven-major-changes-in-chinas-finalized-personal-information-protection-law/ (Last Access 16/05/2023)

[80] Lee, Alexa, Shi, Mingli, Chen, Qiheng, Horsley, Jamie P., Schaefer, Kendra, Creemers, Rogier, Webster, Graham, *Seven Major Changes in China's Finalized Personal Information Protection Law*, DigiChina, Stanford University, 15/09/2021. Available at: https://digichina.stanford.edu/work/seven-major-changes-in-chinas-finalized-personal-information-protection-law/ (Last Access 16/05/2023)

For what concerns data portability, an analysis of this aspect is necessary before investigating how it was used in the PIPL.

Data portability is the ability to extract their data from one platform or service and store or use it elsewhere.[81]

The right to data portability originates from Article 20 of the GDPR, which states that:

> The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.[82]

Moreover, the second paragraph of the article states that:

> In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.[83]

However, the right to data portability is not absolute, as it is indicated in paragraphs 3 and 4 of the above-mentioned Article, which state that the right to portability shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller[84], and that it shall not adversely affect the rights and freedoms of others.[85]

The right to data portability was not included in the first and second draft, but the final text of the PIPL refers to it in Article 45.

Moreover, the final text of the PIPL also states that where individuals request to transfer their personal information to a personal information handler indicated by them, personal information handlers shall provide a channel to transfer it, as long as the transfer meets conditions set by the CAC.[86]

---

[81] Lee, Alexa, Shi, Mingli, Chen, Qiheng, Horsley, Jamie P., Schaefer, Kendra, Creemers, Rogier, Webster, Graham, *Seven Major Changes in China's Finalized Personal Information Protection Law*, DigiChina, Stanford University, 15/09/2021. Available at: https://digichina.stanford.edu/work/seven-major-changes-in-chinas-finalized-personal-information-protection-law/ (Last Access 16/05/2023)

[82] Art. 20 of General Data Protection Regulation GDPR. Available at: https://gdpr-info.eu/art-20-gdpr/

[83] Ibid.

[84] Ibid.

[85] Ibid.

[86] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

This addition is very relevant to recent Chinese developments in antitrust, as it is widely believed that increasing data portability will enhance market competition, benefitting consumers and fueling innovation.[87]

Although the right to data portability has the mission of protecting personal information, enhancing competition in the data market, and promoting the prosperity of the digital economy, the practical implementation of the right to data portability also faces many practical difficulties[88].

First of all, personal information may be delivered in a format that is neither machine-readable nor easily transferable to a competing firm's products; secondly, smaller firms may face a disproportionately high cost when servicing data portability requests; lastly, the personal information of one person may contain that of another.[89]

Therefore, it can be noted how the realization of the right to data portability is often also operationally complex.[90]

Another important aspect which emerges from the comparison between the two drafts and the final text of the Law regards post-mortem data rights. First of all, the first draft does not deal with such matter. Secondly, the rights included in the second draft of the Law are reduced in the final text: in fact, while the previous draft would have handed the next of kin broad authority to exercise the personal information rights of the deceased, the final version adds language limiting their exercise to "their own lawful, legitimate interests" (*weile zishen de hefa, zhengdan liyi* 为了自身的合法、正当利益) signaling that these rights are not to be abused.[91]

---

[87] Lee, Alexa, Shi, Mingli, Chen, Qiheng, Horsley, Jamie P., Schaefer, Kendra, Creemers, Rogier, Webster, Graham, *Seven Major Changes in China's Finalized Personal Information Protection Law*, DigiChina, Stanford University, 15/09/2021. Available at: https://digichina.stanford.edu/work/seven-major-changes-in-chinas-finalized-personal-information-protection-law/ (Last Access 16/05/2023)

[88] Junhe 君和, "*Gebaofa" Mantan Xilie Zhiyi: Liaoliao Shuju Kexidaiquan Jiang Ruhe Luodi*《个保法》漫谈系列之一：聊聊数据可携带权将如何落地 (*One of a series of talks on the Personal Insurance Law: Talking about how the right to data portability will be implemented*), 22/08/2021. Available at: http://www.junhe.com/legal-updates/1538 (Last Access 28/05/2023).

[89] Lee, Alexa, Shi, Mingli, Chen, Qiheng, Horsley, Jamie P., Schaefer, Kendra, Creemers, Rogier, Webster, Graham, *Seven Major Changes in China's Finalized Personal Information Protection Law*, DigiChina, Stanford University, 15/09/2021. Available at: https://digichina.stanford.edu/work/seven-major-changes-in-chinas-finalized-personal-information-protection-law/

[90] Junhe 君和, 《个保法》漫谈系列之一：聊聊数据可携带权将如何落地 "Gebaofa" Mantan Xilie Zhiyi: Liaoliao Shuju Kexidaiquan Jiang Ruhe Luodi (One of a series of talks on the Personal Insurance Law: Talking about how the right to data portability will be implemented), 22/08/2021. Available at: http://www.junhe.com/legal-updates/1538 (Last Accessed 28/05/2023).

[91] Lee, Alexa, Shi, Mingli, Chen, Qiheng, Horsley, Jamie P., Schaefer, Kendra, Creemers, Rogier, Webster, Graham, *Seven Major Changes in China's Finalized Personal Information Protection Law*, DigiChina, Stanford University, 15/09/2021. Available at: https://digichina.stanford.edu/work/seven-major-changes-in-chinas-finalized-personal-information-protection-law/

Moreover, the final text also adds that an individual can override these next of kin powers by making arrangements before they die[92]; in fact, Article 49 of the Law includes the condition "except where the deceased has arranged otherwise before their death (*sizhe shengqian ling you anpai de chuwai* 死者生前另有安排的除外)[93]".

The last important aspect to focus on when comparing the first draft, the second draft and the final text regards the different obligations for large and small data handlers.

The final text of the Law provides a clearer differentiation between the obligations of large data handlers and smaller data handlers.[94] In particular, the Law imposes extra requirements on large platforms, clarifies regulatory authorities over mobile apps' data activities, and implies smaller operations should be afforded greater flexibility in compliance.[95]

For what concerns large platforms, they were not included in the first draft, while the second draft refers to them as "personal information handlers that provide *basic (jichuxing* 基础性) Internet platform services". By contrast, Article 58 of the final text replaces the adjective *basic* with *important* (*zhongyao* 重要)[96].

In conclusion, from the comparison conducted in this paragraph, it is possible to notice how the final text of the PIPL is the culmination of years of legislative work and policy debate in China[97], and how the latest developments and additions analyzed in this paragraph

[92] Lee, Alexa, Shi, Mingli, Chen, Qiheng, Horsley, Jamie P., Schaefer, Kendra, Creemers, Rogier, Webster, Graham, *Seven Major Changes in China's Finalized Personal Information Protection Law*, DigiChina, Stanford University, 15/09/2021. Available at: https://digichina.stanford.edu/work/seven-major-changes-in-chinas-finalized-personal-information-protection-law/

[93] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[94] Lee, Alexa, Shi, Mingli, Chen, Qiheng, Horsley, Jamie P., Schaefer, Kendra, Creemers, Rogier, Webster, Graham, *Seven Major Changes in China's Finalized Personal Information Protection Law*, DigiChina, Stanford University, 15/09/2021. Available at: https://digichina.stanford.edu/work/seven-major-changes-in-chinas-finalized-personal-information-protection-law/

[95] Ibid.

[96] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[97] Lee, Alexa, Shi, Mingli, Chen, Qiheng, Horsley, Jamie P., Schaefer, Kendra, Creemers, Rogier, Webster, Graham, *Seven Major Changes in China's Finalized Personal Information Protection Law*, DigiChina, Stanford University, 15/09/2021. Available at: https://digichina.stanford.edu/work/seven-major-changes-in-chinas-finalized-personal-information-protection-law/

are the results of an ongoing policy thinking and debate[98], and of continuous efforts to keep up with the technological developments.

Moreover, the result of the amendments in the final version of the PIPL is that the law is now less ambiguous, and it gives stronger protection to data subjects, as almost all of the changes detailed above benefit data subjects.[99]

1.3 Purpose, objectives, and key points of the Law

Now that the historical and regulatory background of the PIPL, as well as the two drafts which led to the final text of the Law have been fully investigated, a focus on the PIPL's purpose, objective and key points is necessary.

Before moving to the analysis of the key points, a brief introduction to the Law's structure is worth a mention.

The PIPL consists of seventy-three articles divided into seven chapters, which deal with general provisions, personal information handling rules, the cross-border data transfer rules, individuals rights in personal information handling activities, personal information handlers' duties, the departments fulfilling personal information protection duties, legal liability, and supplemental provisions.

First of all, the purpose of the Law is defined by Article 1, which states that:

> This Law is formulated, on the basis of the Constitution, in order to protect personal information rights and interests, standardize personal information handling activities, and promote the rational use of personal information.[100]

Therefore, the PIPL's main focus is individuals' personal information rights and interests, and this aspect is reinforced by Article 2 of the Law which states that individuals' personal

[98] Lee, Alexa, Shi, Mingli, Chen, Qiheng, Horsley, Jamie P., Schaefer, Kendra, Creemers, Rogier, Webster, Graham, *Seven Major Changes in China's Finalized Personal Information Protection Law*, DigiChina, Stanford University, 15/09/2021. Available at: https://digichina.stanford.edu/work/seven-major-changes-in-chinas-finalized-personal-information-protection-law/

[99] Greenleaf, Graham, *China's Completed Personal Information Protection Law: Rights Plus Cyber-security*, 172 Privacy Laws & Business International Report 20-23, UNSW Law Research Paper No. 21-91, 2021, p. 6. http://dx.doi.org/10.2139/ssrn.3989775

[100] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

information receives legal protection, and, as a consequence, no organization or individual can infringe upon individuals' personal information rights and interest[101].

From Article 1 it is also possible to notice that the PIPL can be considered a code of conduct for personal information processing activities.[102]

Moreover, the legislative purpose of the PIPL is not only to protect (*baohu* 保护) personal information, but also to advance the protection and use (*liyong* 利用) of personal information simultaneously.[103]

The second aspect to focus on is the definition of personal information (*geren xinxi* 个人信息), which is defined by Article 4 as:

> all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymization handling.[104]

An important aspect about this definition which should not be underestimated is the exclusion of anonymized information from the category of personal information. In fact, this sentence clarifies that personal information after anonymization handling is not considered as personal information; hence, it is not necessary to apply the provisions of the PIPL to such category of information.[105]

---

[101] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[102] Wang, Chunhui 王春晖, "*Gerenxinxi Baohufa" de Shida Hexin Yaodian Jiexi*《个人信息保护法》的十大核心要点解析 (Analysis of the Ten Core Points of the Personal Information Protection Law.), Zhongguo Dianxin Ye 中国电信业 (China Telecom Industry), 1 (2022): 54-60.

[103] Ibid.

[104] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[105] Wang, Chunhui 王春晖, "*Gerenxinxi Baohufa" de Shida Hexin Yaodian Jiexi*《个人信息保护法》的十大核心要点解析 (Analysis of the Ten Core Points of the Personal Information Protection Law.), Zhongguo Dianxin Ye 中国电信业 (China Telecom Industry), 1 (2022): 54-60.

As indicated by Article 73(4) of the PIPL, anonymization (*niming hua* 匿名化) is the process of personal information undergoing handling to make it impossible to distinguish specific natural persons and impossible to restore.[106]

The term "impossible to restore" (*buneng fuyuan* 不能复原) in this definition can be achieved through two methods: first, deleting the personal description contained in the personal information[107]; second, deleting all identifiers contained in personal information[108].

In addition, the term personal information handling refers to the collection, storage, use, processing, transmission, provision, disclosure, deletion, etc., of personal information.[109]

By looking at the definition of personal information provided by the PIPL, it is possible to notice the influence of the EU General Data Protection Regulation (GDPR). In fact, The PIPL borrows language from the EU GDPR to define personal information as "all information related to identified or identifiable natural persons"[110], which is the same definition provided by Article 4 of the EU regulation.

However, a difference between the two regulations can be noticed in the terms "data" and "information": in fact, while the EU GDPR refers to personal data (that in Chinese would be translated as *shuju* 数据), the PIPL refers to personal information (in Chinese *xinxi* 信息).

Besides the comparison with the PIPL, the definition of personal information provided by Article 4 of the Law also shows that the defining approach of the PIPL goes beyond China's CSL and the Civil Code, which both defined personal information as information that "can identify a natural person directly or in combination with other information".[111]

---

[106] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[107] Wang, Chunhui 王春晖, "*Gerenxinxi Baohufa" de Shida Hexin Yaodian Jiexi*《个人信息保护法》的十大核心要点解析 (Analysis of the Ten Core Points of the Personal Information Protection Law.), Zhongguo Dianxin Ye 中国电信业 (China Telecom Industry), 1 (2022): 54-60.

[108] Ibid.

[109] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[110] *Guide to China's Personal Information Protection Law (PIPL),* Dentons, 30/08/2021. Available at: https://www.dentons.com/en/insights/articles/2021/august/30/guide-to-chinas-personal-information-protection-law (Last Access 20/04/2023)

[111] *Guide to China's Personal Information Protection Law (PIPL),* Dentons, 30/08/2021. Available at: https://www.dentons.com/en/insights/articles/2021/august/30/guide-to-chinas-personal-information-protection-law (Last Access 20/04/2023)

Last definition to analyze is that of personal information handler (*gerenxinxi chulizhe* 个人信息处理者), which is provided by Article 73 of the PIPL.

Personal information handler is defined as:

> any organizations and individuals that, in personal information handling activities, autonomously decide handling purposes and handling methods.[112]

In this case the definition also appears similar to the one provided by the GDPR; however, the two regulations are different, in that the EU regulation distinguishes the role of the PI processor and the PI controller, whereas the PIPL only provides the definition of the PI handler.

Moreover, it is possible to notice that, by using this terminology, the PIPL remains consistent with the Civil Code, which does not adopt the term controller, but only the term handler.[113]

The third aspect to take into consideration is the PIPL's territorial scope, which is defined by Article 3 of the Law. The PIPL not only applies to the handling of personal information within the borders of the PRC, but it also has an extraterritorial scope.

Concerning the processing of personal information within China, regardless of whether the personal information processing is conducted by Chinese companies or local affiliates of multinational corporations, it is subject to the PIPL regulation as long as the organization is based in China.[114]

By contrast, concerning the extraterritorial scope, the application of the PIPL to the personal information handling outside China is subject to a series of circumstances listed in Article 3, which include the purpose of providing products or services to individuals in China; the analysis of individuals' behavior in China; and other circumstances provided by laws and administrative regulations.[115]

---

[112] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[113] *Guide to China's Personal Information Protection Law (PIPL),* Dentons, 30/08/2021. Available at: https://www.dentons.com/en/insights/articles/2021/august/30/guide-to-chinas-personal-information-protection-law (Last Access 20/04/2023)

[114] Ibid.

[115] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

Besides the concepts analyzed above, there are also other key points of the PIPL which are worth an analysis. These aspects will be deeply investigated in chapters II and III of this paper.

In general, an analysis of this Law shows that the PIPL seeks to find a balance between three objectives: protecting individuals from improper data collection and use; stimulating the development of the digital economy, and safeguarding the public interest.[116]

1.4 The separation between privacy *yinsi* 隐私 and personal information *geren xinxi* 个人信息

Compared with other countries, China has established a different system about the link between privacy and personal information through Chinese Civil Code.[117]

In fact, in China, the right to privacy and the right to personal information protection are considered totally different kind of rights[118], and such distinction is clarified in Chapter VI of the Civil Code.

Article 1032 of the Civil Code defines privacy (*yinsi* 隐私) as:

> the undisturbed private life of a natural person and his private space, private activities, and private information that he does not want to be known to others.[119]

[116] Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p. 6. Available at: https://doi.org/10.1093/cybsec/tyac011

[117] Zhang, Lu, *Personal information of privacy nature under Chinese Civil Code*, Computer Law & Security Review, Volume 43, 2021, 105637, ISSN 0267-3649. Available at: https://doi.org/10.1016/j.clsr.2021.105637.

[118] Wang, Yuan, 王苑, *Shuju Quanli Shiye Xia Geren Xinxi Baohu De Quxiang – Yi Gerenxinxibaohu Yu Yinsiquan De Fenli Wei Zhongxin* 数据权力视野下个人信息保护的趋向 ——— 以个人信息保护与隐私权的分立为中心 (*The Trend of Personal Information Protection from the Perspective of Data Power: Centered on the Separation of Personal Information Protection and Privacy Rights.*), Beijing Hangkong Hangtian Daxue Xuebao (Shehui Kexue Ban) 北京航空航天大学学报 (社会科学版) (Journal of Beihang University, Social Science Edition), 35.1 (2022): 45-57.

[119] Zhonghua Renmin Gongheguo Minfadian 中华人民共和国民法典 (Civil Code of the People's Republic of China), 28/05/2020.
http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml

By contrast, Article 1034 of the Civil Code defines personal information (*geren xinxi* 个人信息) as:

> the information recorded electronically or in other ways that can be used, by itself or in combination with other information, to identify a natural person, including the name, date of birth, identification number, biometric information, residential address, telephone number, email address, health information, whereabouts, and the like, of the person.[120]

Moreover, in the Chinese context, a third kind of privacy also exists: the private information which is unwilling to be known to others (*yinmi xinxi* 隐密信息), which is translated as private personal information in the Civil Code. However, it can also be translated as personal information of privacy nature (PIPN).[121]

The Civil Code deepened the relationship between privacy and personal information by regulating the application of the PIPN in Article 1034, which states that private personal information shall be regulated by the provisions on privacy right; where there are no provisions, the provisions on the protection of personal information shall apply.[122]

Some Chinese scholars argue that the main difference between the right to privacy and the personal information is that the former is a kind of passive and defensive rights, which can only make a claim when it is infringed[123]; while the latter is more proactive, and it can be actively controlled and used in digital world.[124]

According to Zhang Lu, the issue of the link between privacy and personal information protection in China can be divided into two phases: the first one is called monism, the second one is called dualism.[125]

The monism phase refers to the period before the Civil Code, when personal information was protected through privacy regulation. The reason was that, due to the similarity between

---

[120] Zhonghua Renmin Gongheguo Minfadian 中华人民共和国民法典 (Civil Code of the People's Republic of China), 28/05/2020.
http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml
[121] Zhang, Lu, *Personal information of privacy nature under Chinese Civil Code*, Computer Law & Security Review, Volume 43, 2021, 105637, ISSN 0267-3649. Available at: https://doi.org/10.1016/j.clsr.2021.105637
[122] 中华人民共和国民法典 Zhonghua Renmin Gongheguo Minfadian (Civil Code of the People's Republic of China) 28/05/2020.
http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml
[123] Zhang, Lu, *Personal information of privacy nature under Chinese Civil Code*, Computer Law & Security Review, Volume 43, 2021, 105637, ISSN 0267-3649. Available at: https://doi.org/10.1016/j.clsr.2021.105637
[124] Ibid.
[125] Zhang, Lu, *Personal information of privacy nature under Chinese Civil Code*, Computer Law & Security Review, Volume 43, 2021, 105637, ISSN 0267-3649. Available at: https://doi.org/10.1016/j.clsr.2021.105637

privacy and personal information, as well as the lack of personal information litigation claim in Chinese law system, plaintiffs usually chose the right to privacy to protect the interest of personal information.[126]

By contrast, the dualism phase refers to the period after the Civil Code, which begins in 2017, when the General Principles of Civil Law 民法总则[127] regulate privacy and personal information into two articles separately (Article 110 and Article 111), and continues with the distinction made in Book IV Chapter 6 of the Civil Code.

Once that a distinction between the two concepts have been provided, it is necessary to highlight both the advantages and disadvantages of this separation.

On the one hand, this separation is beneficial to the correct handling of disputes in practice,

balancing of the protection and use of personal information, and the promotion of the economy development in digital era.[128]

Moreover, the right to privacy generally cannot be processed, as it is a kind of passive right to protect the tranquility of private life, which is closely related to human dignity. Therefore, the separation is beneficial as if treating all personal information as the right to privacy, the needs of interpersonal communication by personal information in lives and the current business practices of the Internet, as well as the value brought by information sharing could be ignored.[129]

On the other hand, this separation also has some drawbacks.

Among them, privacy and personal information are inherently difficult to completely separate, and attempts to distinguish the relationship between the two through the PIPN are not exhaustive in China.[130] Moreover, the concept of PIPN (*yin mi xinxi* 隐密信息) is not mentioned in the PIPL, and this could lead to a greater confusion.

---

[126] Zhang, Lu, *Personal information of privacy nature under Chinese Civil Code*, Computer Law & Security Review, Volume 43, 2021, 105637, ISSN 0267-3649. Available at: https://doi.org/10.1016/j.clsr.2021.105637

[127] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People-s Congress of the PRC), Zhonghua Renmin Gongheguo Minfa Zongze 中华人民共和国民法总则 (General Principles of Civil Law), 15/03/2017. Available at: http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-03/15/content_2018907.htm

[128] Zhang, Lu, *Personal information of privacy nature under Chinese Civil Code*, Computer Law & Security Review, Volume 43, 2021, 105637, ISSN 0267-3649. Available at: https://doi.org/10.1016/j.clsr.2021.105637

[129] Ibid.

[130] Zhang, Lu, *Personal information of privacy nature under Chinese Civil Code*, Computer Law & Security Review, Volume 43, 2021, 105637, ISSN 0267-3649. Available at: https://doi.org/10.1016/j.clsr.2021.105637

In conclusion, it is possible to say that the separation of personal information protection from privacy protection is a technological development.[131]

Moreover, a further distinction between the two rights can be made. While the right to privacy is a communicative behavior between subjects with equal information capabilities[132], personal information protection refers to the processing of personal information by information processors, hence there are not equal information capabilities.

Moreover, the former is a two-way, back-and-forth interaction between two subjects; whereas, the latter is a cold processing imposed by one party on the other.[133]

Such inequality, which characterizes the whole process of personal information processing, will be investigated throughout this paper, as it is crucial to understand the impact of the Law on companies and, in particular, on human resources management.

After an introduction to the PIPL, the following chapter will investigate the impact of the Law on companies, both domestic and foreign.

[131] Wang, Yuan, 王苑, *Shuju Quanli Shiye Xia Geren Xinxi Baohu De Quxiang – Yi Gerenxinxibaohu Yu Yinsiquan De Fenli Wei Zhongxin* 数据权力视野下个人信息保护的趋向 ——— 以个人信息保护与隐私权的分立为中心 (*The Trend of Personal Information Protection from the Perspective of Data Power: Centered on the Separation of Personal Information Protection and Privacy Rights.*), Beijing Hangkong Hangtian Daxue Xuebao (Shehui Kexue Ban) 北京航空航天大学学报 (社会科学版) (Journal of Beihang University, Social Science Edition), 35.1 (2022): 45-57.
[132] Ibid.
[133] Ibid.

Chapter 2. The PIPL's implications for companies

As it was said in the previous chapter, the digitalization, the Internet, and mobile activities, both of individual customers and companies, provide large amounts of unstructured data which can be analyzed and used by companies for achieving better effectiveness and a competitive advantage on the market[134].

As a consequence, the gathering and storage of information is essential to perform companies' activities, e.g., to know as much as possible about a potential customer or to measure an employee's performance. In fact, once individuals' personal information is deeply analyzed, it becomes a basis for formulating business decisions.

Since its date of effectiveness – November 1, 2021 – China's Personal Information Protection Law has had a huge impact on companies, both domestic and international. In particular, this law has a profound effect upon business operations in China with regards to security and privacy management[135]. The impact of the PIPL on the way companies manage their businesses in China is comparable to the one the European GDPR has in the rest of the world. Moreover, given that China has a major share of the global markets, this regulation has implications for global data privacy advocacy.

The PIPL, in conjunction with the Cybersecurity Law (2017) and the Data Security Law (2021), defines the overall cybersecurity and data protection posture of the country and govern the way global organizations operating in China collect, process and share Chinese citizen data[136].

As a consequence, it is extremely important to understand the implications for companies and how they need to manage their resources in order for them to be compliant with it.

To make an example, to be compliant with the PIPL, companies need to make many technical considerations, especially for IT infrastructure and system application and design[137].

---

[134] Bartosik-Purgat, Małgorzata, Ratajczak-Mrożek, Milena, *Big Data Analysis as a Source of Companies' Competitive Advantage: A Review*., Entrepreneurial Business and Economics Review 6.4 (2018): 197-215.
[135] Zhang, Thomas, *Personal Information Protection Law in China: Technical Considerations for Companies,* China Briefing, 23/08/2021. Available at: https://www.china-briefing.com/news/personal-information-protection-law-in-china-technical-considerations-for-companies/ (Last Access: 25/03/2023)
[136] Ghosh, Soumik, *How China's Information Protection Law Affects Businesses*, Bankinfosecurity, 09/09,2021. Available at: https://www.bankinfosecurity.asia/how-chinas-information-protection-law-affects-businesses-a-17498 (Last Access: 17/03/2023)
[137] Zhang, Thomas, *Personal Information Protection Law in China: Technical Considerations for Companies,* China Briefing, 23/08/2021. Available at: https://www.china-briefing.com/news/personal-information-protection-law-in-china-technical-considerations-for-companies/ (Last Access: 25/03/2023)

In order to understand how companies are affected by the PIPL, this chapter will first analyze the chapters and articles of the regulation that concern companies' obligations and requirements. Then, it will focus on the challenges faced by domestic companies and those faced by foreign-invested enterprises (FIEs). Furthermore, it will provide a case study about the Chinese company DiDi Chuxing, which has been profoundly affected by the provisions of this Law.

Last, this chapter will focus on two areas of business which are and will be affected by the PIPL: digital marketing and online advertising.

2.1 Companies' requirements and obligations

Chapter V of the Personal Information Protection Law contains the companies' obligations and requirements. This chapter focuses on personal information handlers' duties and consists of nine articles.

The first article of this chapter – Article 51 – focuses on a series of measures that companies must adopt in order to protect the safety of personal data. Such measures are:

1. Formulating internal management structures and operating rules;
2. Implementing categorized management of personal information;
3. Adopting corresponding technical security measures such as encryption, de-identification, etc.;
4. Reasonably determining operational limits for personal information handling, and regularly conducting security education and training for employees;
5. Formulating and organizing the implementation of personal information security incident response plans;
6. Other measures provided in laws or administrative regulations[138].

[138] Creemers, Rogier, Webster, Graham, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)
Official text in Chinese: Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

The fifth point of the measures mentioned above refers to "personal information security incident response plan". The original text of the law refers to such plans as *geren xinxi anquan shijian yingji yu'an* 个人信息安全事件应急预案, where *yingji yu'an* 应急预案 refers to *incident response plan* or *contingency plan,* which are internal policy guidelines used by companies in case of data security incidents.

Therefore, these plans are tools aimed at helping companies to organize internal departments in order to carry out the necessary measures in an emergency. These emergencies, for instance, include data breaches.

Article 4 of the GDPR defines personal data breach as:

> a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed[139].

The phenomenon of data breach is becoming more and more frequent all around the world, and China is no exception.

In China, the number of data leakage incidents have increased: statistics show that China has ranked third in the world for being targeted by cyber breaches with 51,309,972 data leakage incidents in 2022[140].

Data security incidents in China's data protection legislation refer to cybersecurity incidents (*wangluo anquan shijian* 网络安全事件), data security incidents (*shuju anquan shijian* 数据安全事件) and personal information security incidents (*geren xinxi anquan shijian* 个人信息安全事件).

Personal information security incidents are not directly defined in the PIPL; however, according to the above-mentioned Article 51, they are usually understood as those events that may lead to unauthorized access to personal information or may cause harm to personal information such as leakage, distortion or loss of personal information.[141]

---

[139] General Data Protection Regulation GDPR. Available at: https://gdpr-info.eu/

[140] Zhao Xinhua, Wang Zhefeng, ShanWenyu 赵新华, 王哲峰, 单文钰, *Kuaguo Qiye Shuju Anquan Shijian de Yufang Yu Yingdui (Shangpian) – Fang Zhi Yu Wei Meng, Zhizhi yu Wei Luan* 跨国企业数据安全事件的预防与应对（上篇）——防之于未萌，治之于未乱 (*Prevention and Response to Data Security Incidents of Multinational Enterprises (Part 1)—Preventing the Unseen and Treating the Unsettled*), Jindu Lushi Shiwu Suo 金杜律师事务所 (King&Wood Mallesons), 03/03/2023. Available at: https://www.kwm.com/cn/zh/insights/latest-thinking/prevention-of-data-security-incidents-for-multinational-enterprises.html (Last Access: 19/03/2023)

[141] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

In general, incident response plans should consist of six parts[142]:

1. General principles. They include the purpose of the plan, that is the reasons and objectives for formulating the plan; the laws and regulations on which the plan is based; the scope of application and the working principles.
2. Roles and responsibilities. Emergency response working bodies should be established and their responsibilities should be clarified. In some cases, external experts are hired to assist in these emergency plans.
3. Prevention and early warning mechanism. It is necessary to clarify the data security incident monitoring and reporting mechanism, early warning mechanism and prevention mechanism and to clarify the functions of the monitoring personnel.
4. Emergency response process. The mechanisms of incident notification, classification and grading, emergency initiation, handling and post-disposal should be clarified.
5. Emergency response security measures. Security measures in terms of manpower, materials, technology and funds should be clarified, as well as the responsibilities, and the rewards and punishment mechanisms.
6. Relevant annexes. These include information such as contact information of incident response plan team members, standard operating procedures, etc.

Article 52 states that handlers who process personal information shall designate a *personal information protection officer* (*geren xinxi baohu fuzeren* 个人信息保护负责人) responsible for supervising data processing activities and protective measures adopted[143].

The Article also states that the contact information of the personal information protection officer shall be communicated to the public; and that the name and contact information of this officer shall also be submitted to the authority.

---

[142] For further details, please read: Zhao Xinhua, Wang Zhefeng, ShanWenyu 赵新华, 王哲峰, 单文钰, *Kuaguo Qiye Shuju Anquan Shijian de Yufang Yu Yingdui (Shangpian) – Fang Zhi Yu Wei Meng, Zhizhi yu Wei Luan* 跨国企业数据安全事件的预防与应对（上篇）——防之于未萌，治之于未乱 (*Prevention and Response to Data Security Incidents of Multinational Enterprises (Part 1)—Preventing the Unseen and Treating the Unsettled*), Jindu Lushi Shiwu Suo 金杜律师事务所 (King&Wood Mallesons), 03/03/2023. Available at: https://www.kwm.com/cn/zh/insights/latest-thinking/prevention-of-data-security-incidents-for-multinational-enterprises.html (Last Access: 19/03/2023)

[143]中华人民共和国个人信息保护法 Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (Personal Information Protection Law of the People's Republic of China), 全国人民代表大会 Quanguo Renmin Daibiao Dahui (The National People's Congress of the People's Republic of China), http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml , 20/08/2021.

The figure of the personal information protection officer is similar to the one indicated in the GDPR. The EU regulation defines it as DPO – Data Protection Officer – and analyzes this role, its position and tasks in Articles 38, 39 and 97[144].

Article 53 states that personal information handlers that operate outside the borders of PRC shall establish a dedicated entity (*zhuanmen jigou* 专门机构) or appoint a representative (*zhiding daibiao* 指定代表) within the borders of the People's Republic of China to be responsible to the matters related to the personal information they handle[145].

Moreover, the name and contact methods of the above-mentioned entity or representative must be submitted to the authorities.

A similar notion exists under Article 27 of the GDPR, according to which offshore data processors are required to appoint an EU-based representative. However, this obligation does not apply to:

1. processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or
2. a public authority or body.[146]

Article 54 states that personal information handlers shall regularly engage in audits of their personal information handling and compliance with laws and administrative regulations[147].

---

[144] General Data Protection Regulation GDPR. Available at: https://gdpr-info.eu/

[145] Creemers, Rogier, Webster, Graham, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)
Official text in Chinese: Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[146] General Data Protection Regulation GDPR. Available at: https://gdpr-info.eu/

[147] Creemers, Rogier, Webster, Graham, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)

The term *compliance audit* (*hegui shenji* 合规审计[148]) refers to a comprehensive review of an organization's compliance to laws and regulations.

This aspect is extremely important as, for the first time, the PIPL has included compliance audit of personal information as an obligation into the Chinese law.

In fact, although the compliance audit obligation was first mentioned in Article 11.7 of the "Information Security Technology Personal Information Security Code", which came into effect in October 2020, it is only a recommended national standard at the effectiveness level. This is why we say that only with the PIPL the compliance audit has become an obligation into the Chinese law.

Article 11.7 of the Security Code provides for security audits of personal information processing and includes personal information protection policies, related protocols and security measures as audit objects, and specifies the requirements related to the recording and retention of audit activities[149].

Not only personal information handlers are required to conduct compliance audits to check if their personal information processing activities are compliant on a regular basis, but audit can also be part of an enforcement action. In fact, where the authority discover relatively high risk exists resulting from personal information processing activities, or observe the occurrence of personal information security incidents, it may request the handler to engage professional institutions to conduct compliance audit[150].

---

[148] To read more about compliance audits, please read this research: *Guanyu Tuijin Geren Xinxi Baohu Hegui Shenji de Ruogan Jianyi* 关于推进个人信息保护合规审计的若干建议 (*Some Suggestions on Promoting Compliance Audits of Personal Information Protection*), Geren Xinxi Baohu Hegui Shenji Tuijin Xiaozu 个人信息保护合规审计推进小组 (Personal Information Protection Compliance Audit Promotion Team), December 2021. Available at: https://sjc.nju.edu.cn/_upload/article/files/3f/8e/7c88cdb5453c81bb8ba3c3c7671a/113a2ae6-0d26-4c97-8d5d-6715e94740b8.pdf (Last Access: 21/03/2023)

[149] Cheng Jihong, Liu Lianshi, Wei Longjie 陈际红, 刘连炻, 韦龙杰, *Quanzhi Qingzhong, Duzhi Zhangduan: Ruhe Kaizhan Geren Xinxi Baohufa Xiang Xia de Hegui Shenji?* 权知轻重，度知长短：如何开展《个人信息保护法》项下的合规审计? (*Right to know the weight, right to know the length: How to conduct a compliance audit under the Personal Information Protection Law*?), Zhong Lun 中倫, 10/05/2022. Available at: https://www.zhonglun.com/Content/2022/05-10/1542310423.html (Last Access: 21/03/2023)

[150] Guide to China's Personal Information Protection Law (PIPL), Dentons, 30/08/2021. Available at: https://www.dentons.com/en/insights/articles/2021/august/30/guide-to-chinas-personal-information-protection-law (Last Access 20/04/2023)

The audit under the PIPL is divided into two types: voluntary audit of personal information handlers and mandatory external audit.[151]

The first one is explained in Article 54; the second type is explained in Article 64, according to which, where the supervisory departments discover that large risks exist in personal information handling activities, they can require personal information handlers to entrust specialized institutions to conducts compliance audits of their personal information handling activities.[152]

Article 55 and 56 refer to the personal information protection impact assessment (*geren xinxi baohu yingxiang pinggu* 个人信息保护影响评估). When dealing with this aspect, two questions arise:

a) When is a personal information protection impact assessment required?

b) What issues need to be assessed?

Article 55 provides the answer to the first question, as it indicates that under certain circumstances, handlers shall conduct a personal information protection impact assessment in advance (PIPIA). Such circumstances include:

1. Handling sensitive personal information;
2. Using personal information to conduct automated decision-making;
3. Entrusting personal information handling, providing personal information to other personal information handlers, or disclosing personal information;
4. Providing personal information abroad;
5. Other personal information handling activities with a major influence on individuals[153].

Companies shall conduct a PIPIA before processing data in order to fully identify the risk of data processing, the impact on individuals and check if the security measures are adequate.

---

[151] Cheng Jihong, Liu Lianshi, Wei Longjie 陈际红, 刘连炻, 韦龙杰, *Quanzhi Qingzhong, Duzhi Zhangduan: Ruhe Kaizhan Geren Xinxi Baohufa Xiang Xia de Hegui Shenji?* 权知轻重，度知长短：如何开展《个人信息保护法》项下的合规审计? (*Right to know the weight, right to know the length: How to conduct a compliance audit under the Personal Information Protection Law*?), Zhong Lun 中倫, 10/05/2022. Available at: https://www.zhonglun.com/Content/2022/05-10/1542310423.html (Last Access: 21/03/2023)

[152] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[153] Creemers, Rogier, Webster, Graham, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)

Article 56 provides the answer to the second question, as it defines the content of the personal information protection impact assessment. According to the article, the PIPIA shall cover three main aspects:

1. Whether or not the personal information handling purpose, handling method, etc., are lawful, legitimate, and necessary;
2. The influence on individuals' rights and interests, and the security risks;
3. Whether protective measures undertaken are legal, effective, and suitable to the degree of risk[154].

Moreover, this article indicates that the assessment reports and relevant handling status records shall be retained for at least three years.

Article 57 refers to the hypothesis of personal information leak, distortion or loss and to the measures that shall be adopted by personal information handlers. This phenomenon is also defined as personal data breach incident. Furthermore, this article provides obligations of notifications to the relevant supervisory authorities and the affected individuals. Concerning the notification content, it shall include three elements:

1. The information categories, causes, and possible harm caused by the leak, distortion, or loss that occurred or might have occurred;
2. The remedial measures taken by the personal information handler and measures individuals can adopt to mitigate harm;
3. Contact method of the personal information handler[155].

Moreover, the article states that where measures adopted by companies avoid harm, personal information handlers are allowed not to notify individuals. On the contrary, if the information leaks, loss or distortion creates harm, individuals shall be notified.

Therefore, it is possible to notice that notifying relevant supervisory authority is mandatory, whereas notifying individuals is not.

According to Yingying Zhu 朱颖莹– Partner at Beijing Mingdun Law Firm Beijing *shi ming dun lushi shiwu suo* 北京市铭盾律师事务所 – a solution to minimize data breach problem and consequences is that business have a well-rehearsed data incident response plan

[154] Creemers, Rogier, Webster, Graham, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)
[155] Ibid.

in place, with clear and workable processes and workflows[156]. Moreover, she suggests that companies with everlasting commitments to data security and users' personal data privacy, should have a highly organized, well-tailored, constantly evolving data protection program[157].

By doing so, companies will be able to increase users' trust and loyalty, empower employees and increase competitive advantage.

Article 58 refers to personal information handlers operating important and big Internet platform services, with a large number of users and a complex business model. Such companies shall fulfill four obligations:

1. Establish and complete personal information protection compliance systems and structures according to State regulations, and establish an independent body composed mainly of outside members to supervise personal information protection circumstances;
2. Abide by the principles of openness, fairness, and justice; formulate platform rules; and clarify the standards for intra-platform product or service providers' handling of personal information and their personal information protection duties;
3. Stop providing services to product or service providers on the platform that seriously violate laws or administrative regulations in handling personal information;
4. Regularly release personal information protection social responsibility reports, and accept society's supervision[158].

This aspect was also investigated in EU Digital Market Act and Digital Services Act (DMA/DSA)[159]. Digital Market Act's aim is to ensure that all digital companies, regardless

[156] Zhu, Yingying, *Personal Data Breach Incident Notification under the PIPL*, Mingdun Law Firm, 16/03/2022. Available at: http://en.mdlaw.cn/news_view.aspx?TypeId=5&Id=403&Fid=t2:5:2 (Last Access: 25/03/2023)
[157] Ibid.
[158] Creemers, Rogier, Webster, Graham, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)
Official text in Chinese: Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml
[159] European Union, *Digital Market Act*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925 and European Union, *Digital Services Act*. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022R2065

their size, can compete on a level playing field. Furthermore, this act's purpose is to stop big platforms from imposing unfair conditions on businesses and consumers.

The Digital Services Act aims at creating a safer digital space. To do so, users have the possibility to refuse those options that include profiling. Furthermore, the use of sensitive data (e.g., religion, ethnicity) is not allowed.

In conclusion, the final article of Chapter V of the PIPL – Article 59 – refers to parties that are entrusted to process personal information (*jieshou weituo chuli geren xinxi de weituoren* 接受委托处理个人信息的受托人[160]). Entrusted persons shall adopt necessary measures to ensure the security of the personal information they handle and assist personal information handlers in fulfilling their obligations under the Law.

2.2 Sanctions for the violation of the Law

Administrative punishment is an important way for national government agencies to carry out administrative management, which is conducive to maintaining and ensuring the smooth operation of the national social order. The issue of the allocation of administrative law enforcement jurisdiction, on the other hand, is the prerequisite and basis for imposing administrative penalties on general administrative cases[161].

Administrative punishment is deeply examined in China's Administrative Punishments Law (*Zhonghua Renmin Gongheguo Xingzheng Chufa Fa* 中华人民共和国行政处罚法[162]), which came into force on July 15, 2021.

---

[160] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[161] Jia, Jingxin 贾婧欣, *Qiye Weifa Chuli Geren Xinxi Xingzheng Chufa de Guanxiaquan Zhengyi* 企业违法处理个人信息行政处罚的管辖权争议 (*Jurisdictional disputes over administrative penalties for the handling of personal information by enterprises in violation of the law*), Jingji Yanjiu Daokan 经济研究导刊 (Journal of Economic Research) 19 (2022): 153-55. Available at: https://kns.cnki.net/kcms2/article/abstract?v=P6B9XB_UHltA7AHkgT6aKGT5VUiIdBwI2eq6UI19NMIZYgCU13MGE4yl6x8w1WqAGKJj9KQBSZ_LwcOzkO-TCBeVzaIPosJhMeLdS_8c1wcL_kSFh261eQU2MtdqtpsI&uniplatform=NZKPT

[162] *Administrative Punishments Law of the PRC (2021 edition)*, China Law Translate, 22/01/2021. Available at: https://www.chinalawtranslate.com/en/administrative-punishment-law-2021/#_Toc62220180 (Last Access 23/03/2023) Official text in Chinese: Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), Zhonghua Renmin Gongheguo Xingzheng Chufa Fa 中华人民共和国行政处罚法 (Administrative Punishments Law of the PRC) Available at: http://www.npc.gov.cn/npc/c30834/202101/49b50d96743946bda545ef0c333830b4.shtml

In Article 2 of the Administrative Punishments Law, *administrative punishment* is defined as:

> the actions by administrative organs in accordance with law taken against citizens, legal persons, or other organizations that violate the order of administrative management, to penalize them by methods such as reducing their rights or increasing their obligations[163].

The jurisdiction and management of administrative punishments will be examined in paragraph 2.3 of this chapter.

When examining violations and consequent fines, it is necessary to identify the supervisory authorities. The authorities fulfilling personal information protection duties and responsibilities are explained in Chapter VI of the PIPL.

According to the articles of this chapter, when dealing with supervisory authorities, it is necessary to distinguish the national level and the local level.

At the national level, the Cybersecurity Administration of China (CAC) z*hongguo wangluo Anquan guanli ju* 中国网络安全管理局 is responsible for the overall coordination of personal information protection and related supervision and management. Moreover, the relevant departments of the State Council of the PRC are also responsible for the protection, supervision, and administration of personal information within their respective areas of responsibility, in accordance with the PIPL and other relevant laws and administrative regulations.

At the local level, such duties of protection, supervision, and administration of personal information are determined in accordance with the relevant provisions of State regulation.

On March 7, 2023, during the annual National People's Congress (NPC) sessions *quanguo lianghui* 全国两会, China's State Council announced a plan to establish a National Data Bureau (*guojia shuju ju* 国家数据局).

---

[163] *Administrative Punishments Law of the PRC (2021 edition)*, China Law Translate, 22/01/2021. Available at: https://www.chinalawtranslate.com/en/administrative-punishment-law-2021/#_Toc62220180 (Last Access 23/03/2023)
Official text in Chinese: Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), Zhonghua Renmin Gongheguo Xingzheng Chufa Fa 中华人民共和国行政处罚法 (Administrative Punishments Law of the PRC) Available at: http://www.npc.gov.cn/npc/c30834/202101/49b50d96743946bda545ef0c333830b4.shtml

The new National Data Bureau (NDB) will be responsible for coordinating the integration, sharing, development, and utilization of data resources and pushing forward the planning and building of a digital China, a digital economy, and a digital society[164].

Furthermore, the plan indicated that the new bureau will assume some responsibilities currently managed by the CAC, in particular, the NDB will assume responsibility for coordinating the development, utilization, and sharing of important national data resources, and promoting the exchange of data resources across industries and across departments[165].

In terms of law enforcement, the Personal Information Protection Law indicates the legal liabilities for the violations of the law. Such liabilities are contained in Chapter VII of the PIPL.

The first article of Chapter VII – Article 66 – states that if personal information is handled in violation of the Law, supervisory authorities shall intervene. Authorities shall order correction, confiscate unlawful income and order to suspend or terminate service provision of the application programs unlawfully processing personal information. Where handlers refuse corrections, some fines are imposed: a fine of not more than 1 million Yuan is additionally imposed and responsible persons in charge are fined between 10,000 and 100,000 Yuan. [166]

Article 66 makes a distinction between general circumstances (which are the ones analyzed above) and grave circumstances, which in the original text of the Law are referred to as *qingjie yanzhong de* 情节严重的).

In case of grave circumstances, the consequences of the violations are different. In fact, authorities shall order correction, confiscate unlawful income and impose a fine of not more than 50 million Yuan or 5% of annual revenue. Besides, supervisory authorities may also order the suspension or cessation of relevant business activities for rectification and the revocation of business license.

---

[164] *Data bureau to help build digital society*, The State Council of The People's Republic of China (English.gov.cn), 09/03/2023. Available at: https://english.www.gov.cn/news/topnews/202303/09/content_WS64091edec6d0a757729e7e16.html (Last Access: 22/03/2023)

[165] Yan Luo, Xuezi Dan, Christopher Adams, Sean Stein, *China Reveals Plan to Establish a National Data Bureau*, Global Policy Watch, Covington, 8/03/2023. Available at: https://www.globalpolicywatch.com/2023/03/china-reveals-plan-to-establish-a-national-data-bureau/ (Last Access: 22/03/2023)

[166] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

Under such severe circumstances, not only responsible persons in charge are to be fined between 100,000 and 1 million Yuan, but authorities may also prohibit them from holding high-level positions, e.g., director, supervisor, high-level manager or protection officer. [167]

It is interesting to underline a difference between this Article and GDPR: in fact, unlike the GDPR, the PIPL does not specify whether the annual revenue refers to the worldwide turnover or the revenue generated in China, as the text only refers to *shang yi niandu yingye e* 上一年度营业额, which is translated as *annual revenue*.

By contrast, Article 83(5) of the GDPR specifies that the fine framework can be up to 20 million euros, or in the case of an undertaking, up to 4% of their *total global* turnover of the preceding fiscal year, whichever is higher[168].

Article 67 of the PIPL states that where unlawful acts as provided in the Law occur, they will be entered into credit files as provided by relevant laws and administrative regulations, and be publicized[169].

Given the rising importance of China's credit system, the concept of credit files – *xinyong dangan* 信用档案 – is very important, as these violation records in credit files can have a negative impact on companies' development and reputation.

China's Social Credit System (SCS) *shehui xinyong tixi* 社会信用体系 is used by the Chinese government to score the "creditworthiness" and "trustworthiness" of each individual and organizational actor by a computational score based on their historical and ongoing social and economic activities, and these credit scores will determine whether the actor can obtain benefits or punishments. Through this process, big data innovations and information and communication technologies (ICTs) are rapidly being instrumentalized and

[167] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[168] General Data Protection Regulation GDPR. Available at: https://gdpr-info.eu/

[169] Creemers, Rogier, Webster, Graham, Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)
Official text in Chinese: Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

institutionalized by the government to surveil and govern the political, social, and commercial dominions of China[170].

Furthermore, China's Social Credit System aims to make it easier for people and businesses to make fully-informed business decisions. For instance, a high social credit score will be an indicator that a party can be trusted in a business context.

At first, this system mainly focused on financial creditworthiness, but then it started to encompass a broader notion of trust.

China's SCS supports five goals[171]:

1. Financial creditworthiness *zhengxin* 征信;
2. Judicial enforcement *sifa gongxin* 司法公信;
3. Commercial trustworthiness *shangwu chengxin* 商务诚信;
4. Societal trustworthiness *shehui chengxin* 社会诚信;
5. Government integrity *zhengwu chengxin* 政务诚信.[172]

According to Article 68 of the PIPL, where State organs fail to fulfill personal information protection duties, their superior organs shall order correction. Under the above-mentioned circumstances, this Article also states that the directly responsible persons shall be sanctioned.

Besides, personnel of the authorities performing duties of personal information protection shall be sanctioned if they commit dereliction of duties, abuse their power or engage in favoritism. However, such neglections do not constitute a crime.

Concerning Article 69, it refers to compensation in cases of harm provoked by an unlawful handling of personal information. In case of such unlawful handling of personal

[170] Liang, Fan, Vishnupriya Das, Nadiya Kostyuk, and Muzammil M. Hussain, *Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, Policy and Internet 10.4 (2018): 415-53.

[171] For further details, I suggest reading: Zhonghua Renmin Gongheguo Zhongyang Renmin Zhengfu 中华人民共和国中央人民政府 (Central People's Government of the People's Republic of China), Guowuyuan Guanyu Yinfa Shehui Xinyong Tixi Jianshe Guihua Gangyao (2014-2020 Nian) de Tongzhi 国务院关于印发社会信用体系建设 规划纲要 (2014—2020 年）的通知 (The State Council on the issuance of the social credit system construction. Notice of Planning Outline (2014-2020), 27/06/2014. Available at: http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm

[172] Donnelly, Drew, *China Social Credit System Explained – What is it & How Does it Work?*, Horizons, 06/04/2023. Available at: https://nhglobalpartners.com/china-social-credit-system-explained/ (Last Access: 26/03/2023)

information, where handlers cannot prove they are not at fault, they shall bear compensation and other take responsibility for the infringement[173].

Moreover, in order to determine the compensation for the infringement, two elements shall be taken into consideration: the resulting loss to the individual; and the personal information handlers' resulting benefits. Where neither of them – benefits and loss – can be determined, compensation is calculated according to practical conditions. Hence, it is possible to notice that Article 69 refers to the determination of liability.

Article 70 refers to public interest lawsuits: it states that where a large number of individuals' personal information is handled unlawfully by personal information handlers, the People's Procuratorates and designated authorities may file a lawsuit with a People's Court.

Last article of Chapter VII – Article 71 – states that where a violation of the Law constitutes a violation of public security management, a public security management shall be imposed. Moreover, where the violation of the Law constitutes a crime, criminal liability shall be investigated. [174]

Now that the main sanctions for non-compliance with the Law have been investigated, it is essential to make a comparison between PIPL and GDPR.

Concerning the PIPL, Chapter VII indicates all sanctions for non-compliance with the Law. These sanctions can be summed up into three main points:

a. correction orders, confiscation of unlawful income, provisional suspension, or termination of service;

b. an additional fine of not more than CNY 1,000,000 if correction orders are refused, CNY 50,000,000 (about USD 775,000) in administrative fines or up to 5% of the organization's annual business revenue;

[173] Creemers, Rogier, Webster, Graham, Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)
Official text in Chinese: Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml
[174] Ibid.

c. CNY 1,000,000 (about USD 150,000) in personal administrative fines on the person responsible[175].

Concerning the GDPR, to decide whether and what level of penalty can be imposed, the authorities have a catalogue of criteria which must be taken into consideration for their decision. In particular, GDRP differentiates two kinds of violations: severe and less severe violations.

According to the fourth paragraph of Article 83 of the GDPR, administrative fines up to 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the preceding financial year are imposed if one of the following provisions is infringed:

a) The obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

b) The obligations of the certification body pursuant to Articles 42 and 43;

c) The obligations of the monitoring body pursuant to Article 41(4).[176]

Severe violations are listed in the fifth paragraph of Article 83: administrative fines up to 20 000 000 EUR or up to 4% of the total worldwide annual turnover of the preceding financial year are imposed if one of the following provisions is infringed:

a) The basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

b) The data subjects' rights pursuant to Articles 12 to 22;

c) The transfers of personal data to a recipient in a third country or an international organization pursuant to Articles 44 to 49;

d) Any obligations pursuant to Member State law adopted under Chapter IX;

e) Non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).[177]

Both paragraphs of Article 83 include the sentence “in the case of an undertaking”, and the term *undertaking* requires a deeper analysis.

According to case law of the European Court of Justice:

[175] Polina, Rebeka, *China’s Personal Information Protection Law (PIPL): Is Your Business Ready for It?*, The Sumsuber, 25/01/2022. Available at: https://sumsub.com/blog/china-personal-information-protection-law/#twelfth (Last Access: 22/03/2023)
[176] General Data Protection Regulation GDPR. Available at: https://gdpr-info.eu/
[177] Ibid.

> the concept of an undertaking encompasses every entity engaged in an economic activity, regardless of the legal status of the entity or the way in which it is financed[178].

An undertaking can therefore not only consist of one individual company in the sense of a legal person, but also out of several natural persons or corporate entities. Thus, a whole group can be treated as one undertaking and its total worldwide annual turnover can be used to calculate the fine for a GDPR infringement of one of its companies[179].

In general, an unlawful handling of personal data can be revealed through inspection activities conducted by supervisory authorities, by unsatisfied employees or by customers.

Now that PIPL and GDPR's sanctions have been fully investigated separately, it is necessary to analyze what differentiates these two regulations.

The biggest differences between the consequences for non-compliance in the GDPR and the PIPL can be summed up as follows:

1. The PIPL may impose other penalties in addition to a fine, which could significantly hamper the company's business. These include shutting down access to IT systems or websites, delisting the company's mobile apps from app stores, business suspension, revoking permissions for specific business activities, or in the worst-case scenario, outright revoking the company's business license.[180]
2. The PIPL not only punishes the company, but also the individual who is responsible for PI protection. In the above section on the different PI protection roles, we described the role of "the person in charge of PI protection". Under the PIPL, this person is held equally liable for non-compliance as the company and could be fined as much as RMB 1 million (~US$150,000) for transgressions. Moreover, they can be prohibited from taking up the role of a senior executive or the person in charge of PI protection for a certain period of time[181].

To sum up what we have seen in this paragraph, it can be seen that in terms of legal liability, the PIPL regulates multiple dimensions such as administrative punishment, civil compensation, and criminal liability. In particular, in terms of administrative penalties, not

[178] *General Data Protection Regulation GDPR Fines/Penalties*, Intersoft Consulting. Available at: https://gdpr-info.eu/issues/fines-penalties/#:~:text=83(4)%20GDPR%20sets%20forth,fiscal%20year%2C%20whichever%20is%20higher (Last Access 22/03/2023)
[179] Ibid.
[180] Zhang, Thomas, *GDPR Versus PIPL – Key Differences and Implications for Compliance in China,* China Briefing, 18/05/2022. Available at: https://www.china-briefing.com/news/pipl-vs-gdpr-key-differences-and-implications-for-compliance-in-china/ (Last Access: 22/03/2023)
[181] Ibid.

only can the enterprise itself be punished (up to 5% of the previous year's turnover), but also the directly responsible managers and other responsible personnel can be fined nearly one million, which undoubtedly makes the compliance needs of enterprises in personal information protection more urgent[182].

Last aspect to be mentioned when dealing with PIPL's sanctions is that foreign companies managing personal information within the borders of PRC have to deal with additional sanctions. These sanctions will be analyzed in the following paragraph.

2.2.1. Sanctions for foreign companies

Besides all the sanctions stated in Chapter VII of the PIPL, additional penalties are imposed to foreign companies that handle Chinese citizens' personal information outside the borders of PRC.

These sanctions are included in Article 42 of Chapter III of the Law.

This Article states that where foreign organizations handle personal information violating personal information rights and interests of citizens of the People's Republic of China, or harming the national security or public interest of the People's Republic of China, the State cybersecurity and informatization department may put them on a list limiting or prohibiting personal information provision, issue a warning, and adopt measures such as limiting or prohibiting the provision of personal information to them, etc.[183]

It means that foreign companies handling personal information which do not comply with the PIPL and harm China's national security shall be put on a block list and prohibited from handling Chinese citizens' personal information. However, the PIPL does not clarify what constitutes a violation of Chinese citizens' personal information rights or what qualifies as harming China's national security or public interest.

---

[182] *Geren Xinxi Baohufa Dui Qiye de Shi Da Yingxiang*《个人信息保护法》对企业的十大影响 (*Ten Big Effects of the Personal Information Protection Law on Enterprises*), Zhongguo Zhongxiao Qiye Guoji Hezuo Xiehui 中国中小企业国际合作协会 (International Cooperation Association of SMEs), 27/8/2021. Available at: https://xiehui.chinasme.org.cn/site/content/8594.html (Last Access: 24/03/2023)

[183] Creemers, Rogier, Webster, Graham, Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)
Official text in Chinese: Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

In conclusion, the Personal Information Protection Law has put forward higher requirements for the protection of personal information, and each company – either domestic or foreign – should pay attention to its impact on the compliance work of the company, so as to effectively avoid risks and guarantee the normal operation and sustainable development of the company.[184]

2.3 Companies' illegal handling of personal information and the allocation of jurisdiction for administrative penalties

Illegal handling of personal information by enterprises refers to the arbitrary collection, illegal acquisition, excessive use and illegal trading of personal information, and the use of personal information to disrupt and endanger people's lives, health and property security[185]. For instance, when applications in people's mobile phones are in silent state, personal information – e.g., pictures, audio – are collected; or when people purchase items or services on online platforms, users' shopping information can be collected to customize advertisements.

Moreover, an increasing number of companies use big data to analyze and evaluate customers for marketing purposes. They evaluate customers' tastes and habits by having information about their consumption habits, economic status, price sensitivity and so on. Among these companies, some manage users' personal information in an unlawful manner. For instance, they do not fulfill their obligations to protect personal information causing a leak of personal information or they even sell personal information to increase their profit. The growing value and importance of big data represents the reason why nowadays it is said that data is the new gold, or even the new oil.

---

[184] *Geren Xinxi Baohufa Dui Qiye de Shi Da Yingxiang*《个人信息保护法》对企业的十大影响 (*Ten Big Effects of the Personal Information Protection Law on Enterprises*), Zhongguo Zhongxiao Qiye Guoji Hezuo Xiehui 中国中小企业国际合作协会 (International Cooperation Association of SMEs), 27/8/2021. Available at: https://xiehui.chinasme.org.cn/site/content/8594.html (Last Access: 24/03/2023)

[185] 贾婧欣 Jia, Jingxin. "企业违法处理个人信息行政处罚的管辖权争议 Qiye Weifa Chuli Geren Xinxi Xingzheng Chufa de Guanxiaquan Zhengyi." (Jurisdictional disputes over administrative penalties for the handling of personal information by enterprises in violation of the law) 经济研究导刊 Jingji Yanjiu Daokan (Journal of Economic Research) 19 (2022): 153-55. Available at: https://kns.cnki.net/kcms2/article/abstract?v=P6B9XB_UHltA7AHkgT6aKGT5VUiIdBwI2eq6UI19NMIZYgCU13MGE4yl6x8w1WqAGKJj9KQBSZ_LwcOzkO-TCBeVzaIPosJhMeLdS_8c1wcL_kSFh261eQU2MtdqtpsI&uniplatform=NZKPT

To respond to such unlawful situations, relevant authorities actively try to take severe measures against illegal behavior of companies, they pursue civil liability for the infringement of the enterprise or maintain civil rights and legal authority through administrative punishment[186].

According to Jingxin Jia 贾婧欣, the illegal handling of personal information by enterprises has peculiar and unique characteristics. In fact, three main characteristics emerge:

1. Due to the virtual nature of personal information, the illegal handling of personal information by enterprises also exists in the virtual space. As a consequence, it is difficult to identify accurately the infringers when users' personal information rights are violated.

2. The immediacy of information dissemination makes it difficult for companies to illegally process personal information. The scope of harm is easily expanded and the impact is extensive. Moreover, with the advancement of network technology and the prosperity and development of APP, the problems of personal information leakage, abuse and illegal transactions have become increasingly prominent.

3. Cases of illegal handling of personal information by enterprises mostly occur in the cyberspace.

Compared with the real world, cyberspace is relatively free and not restricted by abstract norms, so the incidence of illegal activities is higher. In 2021, the network security department of the public security organ strengthened the protection of citizens' personal information, investigated and dealt with as many as 386 APP service units that violated laws and regulations to collect citizens' personal information.

Among them, 97 were subject to administrative penalties, 192 were ordered to rectify according to law, and 51 were shut down[187].

---

[186] Jia, Jingxin 贾婧欣, *Qiye Weifa Chuli Geren Xinxi Xingzheng Chufa de Guanxiaquan Zhengyi* 企业违法处理个人信息行政处罚的管辖权争议 (*Jurisdictional disputes over administrative penalties for the handling of personal information by enterprises in violation of the law*), Jingji Yanjiu Daokan 经济研究导刊 (Journal of Economic Research) 19 (2022): 153-55. Available at: https://kns.cnki.net/kcms2/article/abstract?v=P6B9XB_UHltA7AHkgT6aKGT5VUiIdBwI2eq6UI19NMIZYgCU13MGE4yl6x8w1WqAGKJj9KQBSZ_LwcOzkO-TCBeVzaIPosJhMeLdS_8c1wcL_kSFh261eQU2MtdqtpsI&uniplatform=NZKPT

[187] Jia, Jingxin 贾婧欣, *Qiye Weifa Chuli Geren Xinxi Xingzheng Chufa de Guanxiaquan Zhengyi* 企业违法处理个人信息行政处罚的管辖权争议 (*Jurisdictional disputes over administrative penalties for the handling of personal information by enterprises in violation of the law*), Jingji Yanjiu Daokan 经济研究导刊 (Journal of Economic Research) 19 (2022): 153-55. Available at: https://kns.cnki.net/kcms2/article/abstract?v=P6B9XB_UHltA7AHkgT6aKGT5VUiIdBwI2eq6UI19NMIZYgCU13MGE

In her paper, Jia Jingxin 贾婧欣 also analyzed the relationship between PIPL and China's administrative penalty jurisdiction system.

The jurisdiction of administrative punishment aims to solve the problem of which type, level and place of administrative organs specifically exercise the jurisdiction of administrative punishments and can be divided into functional jurisdiction, hierarchical jurisdiction and territorial jurisdiction[188].

Functional jurisdiction refers to the division of authority among the functional administrative organs in administrative punishment cases according to the administrative legal norms violated by the illegal acts in the administrative punishment cases and the professional nature and departmental attributes of the administrative punishment to be imposed.

Hierarchical jurisdiction refers to the division of authority between the upper and lower functional agencies with the same function, between the upper- and lower-people's governments, and between the people's governments at all levels and their functional agencies for the initial investigation and handling of administrative punishment cases.

Territorial jurisdiction refers to the determination of the division of labor and authority for the first handling of administrative affairs between administrative entities at the same level in the administrative entity system.

However, in order to improve the jurisdiction of administrative punishment and form a complete jurisdictional system, China has also developed special rules such as transfer jurisdiction, designated jurisdiction and duty assistance.[189]

Through a deep analysis, Jia Jingxin 贾婧欣 has noticed that although the introduction of the Personal Information Protection Law has drawn a red line for the handling of personal

4yl6x8w1WqAGKJj9KQBSZ_LwcOzkO-TCBeVzaIPosJhMeLdS_8c1wcL_kSFh261eQU2MtdqtpsI&uniplatform=NZKPT

[188] Jiang, Bixin 江必新, *Xingzheng Chufa Fa Tiaowen Jingshi Yu Shili Jingjie* 行政处罚法条文精释与实例精解, (*Detailed interpretation of the provisions and examples of the Administrative Punishment Law*) Beijing 北京: Renmin Fayuan Chubanshe 人民法院出版社 (People's Court Press), 2021: 7.

[189] Jia, Jingxin 贾婧欣, *Qiye Weifa Chuli Geren Xinxi Xingzheng Chufa de Guanxiaquan Zhengyi* 企业违法处理个人信息行政处罚的管辖权争议 (*Jurisdictional disputes over administrative penalties for the handling of personal information by enterprises in violation of the law*), Jingji Yanjiu Daokan 经济研究导刊 (Journal of Economic Research) 19 (2022): 153-55. Available at: https://kns.cnki.net/kcms2/article/abstract?v=P6B9XB_UHltA7AHkgT6aKGT5VUiIdBwI2eq6UI19NMIZYgCU13MGE4yl6x8w1WqAGKJj9KQBSZ_LwcOzkO-TCBeVzaIPosJhMeLdS_8c1wcL_kSFh261eQU2MtdqtpsI&uniplatform=NZKPT

information by companies, it is necessary to solve the problem of its connection with traditional laws in order for the law to be truly implemented.

Once the unlawful handling of personal information by enterprises and the allocation of jurisdiction for administrative penalties have been investigated, it is necessary to focus on how Chinese companies are affected by the PIPL.

2.4. The PIPL's impact on Chinese companies

After its implementation, the Personal Information Protection Law has become the *san jia ma che* 三驾马车 – the troika[190] – of China's cyberspace management and data protection, together with the Cybersecurity Law (2017) and the Data Security Law (2021).[191]

As Li Yiqiang – Partner in Faegre Drinker – states, these three laws have significantly tightened Chinese government's control over data privacy in China and revealed the government's determination to assert data sovereignty over cross-border data transfers.[192]

As a consequence, China's Personal Information Protection Law has a huge impact on how companies do business within the borders of PRC.

China International Cooperation Association of SMEs (CICASME) *zhongguo zhongxiao qiye guoji hezuo xiehui* 中国中小企业国际合作协会 was founded in 1990, and it is the first national SME social organization in China, co-located and closely cooperating with the SME Development Promotion Center of the Ministry of Industry and Information Technology.

The Association has developed into a social organization with the most authoritative status, the most standardized operation, the widest contact and the greatest international influence in the field of Chinese SMEs[193].

Among its main purposes, the CICASME aims to build international cooperation zones for Chinese and foreign SMEs. In fact, by taking advantages of international cooperation, it

---

[190] A group of three (e.g., countries, organizations, politicians).

[191] *Geren Xinxi Baohufa Dui Qiye de Shi Da Yingxiang*《个人信息保护法》对企业的十大影响 (*Ten Big Effects of the Personal Information Protection Law on Enterprises*), Zhongguo Zhongxiao Qiye Guoji Hezuo Xiehui 中国中小企业国际合作协会 (International Cooperation Association of SMEs), 27/8/2021. Available at: https://xiehui.chinasme.org.cn/site/content/8594.html (Last Access: 24/03/2023)

[192] Li, Yiqiang, *Challenges Under New Personal Information Protection Regime in China*, Faegre Drinker, 25/8/2021. Available at: https://www.faegredrinker.com/en/insights/publications/2021/8/challenges-under-new-personal-information-protection-regime-in-china (Last Access: 26/03/2023)

[193] Zhongguo Zhongxiao Qiye Guoji Hezuo Xiehui, Guanyu Xiehui 中国中小企业国际合作协会，关于协会, (China International Cooperation Association of SME, About us). Available at: https://xiehui.chinasme.org.cn/site/content/7373.html (Last Access: 02/04/2023)

has attracted more than 2,000 high-quality foreign-funded enterprises to settle in the zone.[194] This is why the organization's name includes the term *guoji hezuo* 国际合作, which means "international cooperation".

The CICASME has identified ten major impacts of PIPL on enterprises, which will be described below.

1) Enterprises should pay attention to the rights and interests of personal information and to the extraterritorial application.

As it was said in Chapter I of this paper, the activity of personal information handling includes the collection, storage, use, processing, transmission, provision, disclosure, deletion of personal information.[195]

When they are involved in personal information handling activities – for instance, using, processing and transmitting data – enterprises shall pay close attention to the rights and interests of personal information and prevent infringement, e.g., data leakage or excessive collection of data; otherwise, enterprises shall bear administrative, civil and criminal liabilities.

Concerning the jurisdictional application, companies should note that the PIPL applies not only to activities of handling individuals' personal information within the borders of PRC, but also to those which occur outside China. As a consequence, those companies with cross-border business activities shall adopt additional measures in order to be compliant with the Law.

2) Enterprises shall observe seven principles when handling personal information.

When handling personal information, companies shall observe seven principles which are defined in the following articles of the PIPL:

1. Article 5: follow the principles of legality, propriety, necessity and good faith;

[194] Zhongguo Zhongxiao Qiye Guoji Hezuo Xiehui, Guanyu Xiehui 中国中小企业国际合作协会，关于协会, (China International Cooperation Association of SME, About us). Available at: https://xiehui.chinasme.org.cn/site/content/7373.html (Last Access: 02/04/2023)

[195] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

2. Article 6: follow the purpose limitation principle. Personal information handling shall have a clear and reasonable purpose;

3. Article 6: follow the principle of minimum necessity. Handlers shall adopt a method that has the least impact on personal rights and interests and that shall be limited to the minimum scope of achieving the purpose of processing, and must not collect excessive personal information;

4. Article 7: follow the principle of openness and transparency. The purpose, method and scope of handling shall be clearly indicated. In addition, the rules for handling personal information shall be disclosed;

5. Article 8: follow the quality principle. Handlers shall ensure the quality of personal information;

6. Article 9: follow the principle of accountability. Handlers shall be responsible for their personal information processing activities;

7. Article 9: follow the principle of data security. Handlers shall take necessary measures to ensure the security of the personal information processed[196].

The observation of these seven principles is the basic condition for personal information handlers.

Besides the above-mentioned principles, another basic requirement for enterprises in the collection and handling of data is included in Article 10 of the PIPL. According to this Article, when collecting and processing data, enterprises shall not illegally collect, use, process or transmit personal information of others, or illegally trade, provide or disclose personal information of others, or engage in personal information processing activities that endanger national security or public interests[197].

[196] *Geren Xinxi Baohufa Dui Qiye de Shi Da Yingxiang*《个人信息保护法》对企业的十大影响 (*Ten Big Effects of the Personal Information Protection Law on Enterprises*), Zhongguo Zhongxiao Qiye Guoji Hezuo Xiehui 中国中小企业国际合作协会 (International Cooperation Association of SMEs), 27/8/2021. Available at: https://xiehui.chinasme.org.cn/site/content/8594.html (Last Access: 24/03/2023)

[197] Creemers, Rogier, Webster, Graham, Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)

3) Enterprises should distinguish the different situations of informed consent.

Enterprises can only process personal information with the consent of the individual, which is the embodiment of the core principle of "inform and consent[198]".

Enterprises should also pay attention to two other elements: separate consent or written consent. According to Article 14 of the Law, where laws and administrative regulations provide that the individual's separate consent or written consent shall be obtained for the processing of personal information, those provisions shall be followed[199].

This puts forward higher requirements for informed consent under special circumstances, e.g., the collection of minors' personal information requires the consent of their parents or other guardians.

However, it according to Article 13 of the Personal Information Protection Law, there are other special circumstances that do not require the consent of the individual, these include:

1. The conclusion and performance of a contract to which the individual is a party;
2. The implementation of human resources management in accordance with the labor rules and regulations formulated in accordance with the law and the collective contract signed in accordance with the law;
3. The performance of statutory duties or legal obligations;
4. When it is necessary to respond to public health emergencies or protect the life, health and property safety of natural persons in an emergency;
5. For the implementation of news reporting, public opinion supervision, etc;
6. For personal information disclosed by persons themselves or otherwise already lawfully disclosed[200].

Moreover, enterprises shall pay attention to the situation in which informed consent is required, and where the purpose of processing personal information, the method of processing, and the type of personal information to be processed changes. Under this circumstance, the individual's consent shall be re-obtained (Article 14).

---

[198] *Geren Xinxi Baohufa Dui Qiye de Shi Da Yingxiang*《个人信息保护法》对企业的十大影响 (*Ten Big Effects of the Personal Information Protection Law on Enterprises*), Zhongguo Zhongxiao Qiye Guoji Hezuo Xiehui 中国中小企业国际合作协会 (International Cooperation Association of SMEs), 27/8/2021. Available at: https://xiehui.chinasme.org.cn/site/content/8594.html (Last Access: 24/03/2023)

[199] Creemers, Rogier, Webster, Graham, Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)

[200] Ibid.

An additional aspect to be considered is the individuals' right to withdraw consent. In fact, according to Article 15, if personal information is processed based on the individual's consent, the individual has the right to withdraw his consent, and the personal information processor shall provide a convenient way to withdraw consent. In the case of withdrawal of consent, the withdrawal of consent by an individual does not affect the validity of personal information processing activities already carried out based on the individual's consent before the withdrawal[201].

Although individuals' consent and right to withdraw consent are crucial elements for the handling of personal information, Article 16 states that where an individual does not consent to the processing of his or her personal information or withdraws consent, the personal information processor shall not refuse to provide products or services on this basis, except where the processing of personal information is necessary for the provision of products or services[202].

As a consequence, companies shall provide their product or service to individuals even without their consent. The only exception is when the service provided fully depends on the handling of personal information.

To sum up, when dealing with individuals' consent, companies shall be able to distinguish four main situations: when individuals' consent is fundamental for processing data; when individuals' consent is not required; when separate consent shall be re-obtained; when individuals decide to withdraw consent.

4) Enterprises shall bear different responsibilities in joint processing and entrusted processing.

Companies' responsibilities in joint processing and entrusted processing are described in Articles 20, 21, 22, 23 of the PIPL.

Joint processing occurs when two or more personal information processors jointly decide (*gongtong jueding* 共同决定) on the purpose and method of processing personal information. In this case, according to Article 20, the two or more parties shall agree on their respective rights and obligations.

[201] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml
[202] Ibid.

However, this agreement does not affect an individual's request to any of the personal information processors to exercise the rights provided for in the Law.[203]

In the case of joint processing, user has the right to exercise rights against either party, and the contract can only be effective within the cooperative enterprise. In addition, Article 20 also states that where the infringement of personal information rights and interests causes damage, the enterprise shall bear joint liability (*liandai zeren* 连带责任) according to the Law.[204]

Entrusted processing (*weituo chuli* 委托处理) occurs when the personal information processor entrusts the handling of personal information. In this case, Article 21 states that the handler shall agree with the trustee on the purpose, period, and method of handling, the types of personal information, protection measures, and the rights and obligations of both parties, and supervise the trustee's personal information processing activities.[205]

Moreover, entrusted persons shall handle personal information in accordance with the agreement, and must not process personal information beyond the agreed processing purpose, processing method, etc., in excess of the agreement.[206]

Where the entrustment contract is not effective, invalid, revoked, or terminated, the trustee shall return the personal information to the personal information processor or delete it, and must not retain it. This imposes corresponding compliance requirements on the data activities of both the principal and the trustee.[207]

---

[203] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[204] Ibid.

[205] Ibid.

[206] Creemers, Rogier, Webster, Graham, Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)

[207] *Geren Xinxi Baohufa Dui Qiye de Shi Da Yingxiang*《个人信息保护法》对企业的十大影响 (*Ten Big Effects of the Personal Information Protection Law on Enterprises*), Zhongguo Zhongxiao Qiye Guoji Hezuo Xiehui 中国中小企业国际合作协会 (International Cooperation Association of SMEs), 27/8/2021. Available at: https://xiehui.chinasme.org.cn/site/content/8594.html (Last Access: 24/03/2023)

The third circumstance that requires an analysis is the transfer of personal information due to merger, division, dissolution or declaration of bankruptcy. In these cases, according to Article 22 of the PIPL, companies shall notify the individual about the receiving party's name and contact information. In addition, the receiving party shall continue to perform the obligations of the personal information processor. Where the receiving party changes the original purpose or method of processing, the individual shall be notified.

The fourth and last case to investigate concerns when enterprises provide other personal information processors with the personal information they handle. Under this circumstance, Article 23 of the Law states that handlers shall inform the individual of the name of the recipient, contact information, purpose of processing, processing methods, and types of personal information, and obtain the individual's separate consent. The receiving party shall process personal information within the scope of the above processing purposes, processing methods, and types of personal information. Where the receiving party changes the original purpose or method of processing, it shall re-obtain the individual's consent in accordance with the provisions of the Law. [208]

5)Enterprises should avoid big data killing and standardize automated decision-making.

Big data killing (*da shuju shashu* 大数据杀熟) refers to the phenomenon of companies using big data to analyze the daily consumption habits of consumers in order to set different prices to different consumers, which is called price discrimination in economics.[209]

Big data killings occur in the field of Internet e-commerce, causing damage to consumers' rights and interests and having a very negative impact.

Article 24 of the PIPL regulates it, as it states that personal information handlers using personal information to conduct automated decision-making shall ensure the transparency of decision-making and the fairness and impartiality of the results, and shall not engage in

[208] Creemers, Rogier, Webster, Graham, Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)

[209] Chen, Jiayao, *Economic Thinking of Big Data Killing in the Internet Era*, 2021, In: Abawajy, J., Choo, KK., Xu, Z., Atiquzzaman, M. (eds) 2020 International Conference on Applications and Techniques in Cyber Intelligence. ATCI 2020. Advances in Intelligent Systems and Computing, vol 1244. Springer, Cham. https://doi.org/10.1007/978-3-030-53980-1_142

unreasonable differential treatment of individuals in transaction conditions such as trade prices.

Automated decision-making (*zidonghua juece* 自动化决策) is defined in Article 73 of the Law as:

> the activity of using computer programs to automatically analyze or assess personal behaviors, habits, interests, or hobbies, or financial, health, credit, or other status, and make decisions based thereupon.[210]

Moreover, Article 24 also states that if handlers conduct information push delivery and commercial sales to individuals through automated decision-making, they shall also provide options that do not target their personal characteristics, or provide individuals with convenient ways to refuse. That is, for enterprises, in addition to the advertising business model of personalized push, it is also necessary to provide non-personalized and rejectable options[211].

In addition, individuals have the right to request explanations from personal information handlers, and to refuse that personal information handlers make decisions only through automated decision-making when enterprises use automated decision-making that has a significant impact on individuals' rights and interests. Therefore, enterprises should be able to identify decision-making situations that have significant impact and give users the right to refuse.

6)Enterprises should strictly limit the processing of sensitive personal information.

Sensitive personal information is included in Section II of the PIPL and, according to Article 28 of the Law, it can be defined as personal information that if leaked or illegally used can cause harm to the dignity of individuals or endanger personal and property safety.

Therefore, PIPL stipulates that personal information handler can only process sensitive personal information if there is a specific purpose and sufficient necessity, and strict

[210] Creemers, Rogier, Webster, Graham, Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)

[211] *Geren Xinxi Baohufa Dui Qiye de Shi Da Yingxiang*《个人信息保护法》对企业的十大影响 (*Ten Big Effects of the Personal Information Protection Law on Enterprises*), Zhongguo Zhongxiao Qiye Guoji Hezuo Xiehui 中国中小企业国际合作协会 (International Cooperation Association of SMEs), 27/8/2021. Available at: https://xiehui.chinasme.org.cn/site/content/8594.html (Last Access: 24/03/2023)

protection measures are taken. Moreover, for the processing of sensitive personal information the separate consent of the individual shall be obtained. In some cases, for instance where laws and administrative regulations provide it, written consent shall also be obtained.

In addition, according to Article 30, when handling sensitive personal information, handlers shall inform individuals not only of the general matters, but also of the necessity of handling sensitive personal information and the impact on individuals' rights and interests.

In conclusion, personal information of minors under the age of 14 is also considered sensitive personal information. As a consequence, as it is indicated in Article 31, to process personal information of minors under the age of 14, companies shall obtain the consent of the minor's parents or other guardians, and for such information, enterprises shall also formulate special personal information processing rules.[212]

7)Enterprises should pay attention to the rules on cross-border provision of personal information.

Rules on cross-border provision of personal information are included in Chapter III of the PIPL. Chapter III defines the conditions that shall be met by companies that handle Chinese citizens' personal information outside the borders of PRC. These provisions mainly affect those companies with business overseas, rather than the domestic ones.

Companies shall adopt any measure to be compliant with these regulations in order to avoid penalties, e.g., high fines or being added to a black list.

However, Chapter III of the PIPL and all the provisions on cross-border data transfer will be analyzed in Chapter II of this thesis.

8)Enterprises should pay attention to individuals' rights in personal information handling activities.

Individuals' rights in personal information handling activities are listed in Chapter IV of the PIPL. When handling personal data, all companies must not underestimate this aspect.

[212] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

According to Chapter IV of the Law, there are ten individuals' rights that must be considered when handling personal information.

Article 44 states that individuals have the right to know and the right to decide relating to their personal information. Moreover, they also have the right to limit or refuse the handling of personal information.[213]

Article 45 states that individuals have the right to consult and copy their personal information from personal information handlers.[214] The only exceptions are circumstances listed in Article 18 and Article 35 of the PIPL.

To comply with this aspect, companies shall develop a privacy interface. A privacy interface is important for implementing privacy principles and protecting user rights.

It also makes the data lifecycle transparent to users, allowing them to control what data is being used and how it is being processed, and access a copy of the collected data.[215]

Moreover, this Article also indicates individuals' right of portability, that is personal information processors shall provide channels for transferring personal information to the personal information processors designated by them if individuals require to do so.

According to Article 46, individuals have the right to request that personal information handlers correct or complete their personal information if they notice that their personal data is incorrect or incomplete.

Article 47 indicates a list of five circumstances under which individuals have the right to request the deletion of their personal information. Such circumstances are:

> 1. The handling purpose has been achieved, is impossible to achieve, or [the personal information] is no longer necessary to achieve the handling purpose;
> 2. Personal information handlers cease the provision of products or services, or the retention period has expired;
> 3. The individual rescinds consent;
> 4. Personal information handlers handled personal information in violation of laws, administrative regulations, or agreements;

---

[213] Creemers, Rogier, Webster, Graham, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)

[214] Ibid.

[215] Zhang, Thomas, *Personal Information Protection Law in China: Technical Considerations for Companies*, China Briefing, 23/08/2021. Available at: https://www.china-briefing.com/news/personal-information-protection-law-in-china-technical-considerations-for-companies/ (Last Access: 25/03/2023)

5. Other circumstances provided by laws or administrative regulations[216].

Concerning individuals' rights listed in Articles 45 and 47, companies need to consider how to quickly locate each user's personal information within the IT system and predefine a way of exporting a copy and delivering it to the user. Moreover, they also need to consider ways of making each user's record 'independent' to ensure that the deletion of one user's record will not impact other existing or in-use data.[217]

Furthermore, enterprises also need to plan for a reasonable authentication mechanism to accurately recognize the user who makes an inquiry or requests a copy, update, or deletion. In this case, the adjective *reasonable* means striking a balance between collecting enough personal identification information to authenticate the user and hedging against the increased risks associated with being responsible for larger amounts of potentially sensitive data[218].

Moreover, the right to deletion requires the company to consider the deployment of a universal platform for saving related personal data, so that the data can be easily located and deleted from all locations. A common issue that can arise in practice is data only being deleted from the live system, with another copy kept in the backup system. A predefined retention policy should be considered to delete the data automatically once it has expired, which is a good way to comply the requirements of Article 47(1).[219]

According to Article 48, individuals have the right to know personal information handling rules. As a consequence, handlers shall explain such rules to individuals if requested.

Article 49 states that, where a natural person dies, his or her close relatives may exercise the rights of access, copy, correction, deletion, and other such rights provided for in this

[216] Creemers, Rogier, Webster, Graham, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)
Official text in Chinese: Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml
[217] Zhang, Thomas, *Personal Information Protection Law in China: Technical Considerations for Companies*, China Briefing, 23/08/2021. Available at: https://www.china-briefing.com/news/personal-information-protection-law-in-china-technical-considerations-for-companies/ (Last Access: 25/03/2023)
[218] Ibid.
[219] Ibid.

chapter over the relevant personal information of the deceased[220]. This aspect presents a big challenge for companies as they shall recognize and authenticate a user's closest relative.

To sum up, individuals' rights in personal information handling activities are: right to know and decision, the right to restrict or refuse, the right to access and copy, the right to portability, the right to correction, the right to delete and close relatives' rights of access, copy, correction and deletion.

In conclusion, Article 50 of the Law indicates the personal information handlers' obligations towards individuals' rights. According to this Article, handlers shall establish convenient mechanisms to accept and handle applications from individuals to exercise their rights.[221]

Although handlers can refuse individuals' request, this rejection leads to two consequences: the first is that handlers must explain the reason; the second is that if they reject individuals' requests, individuals have the right to file a lawsuit with a People's Court.

The last two impacts of PIPL on companies are:

9)Enterprises should assume the corresponding obligations as personal information handlers.

10) Enterprises should avoid legal liability for violations of personal information

Unlike the preceding eight ones, these two aspects will not be analyzed in this paragraph, as they were already fully investigated in paragraphs 2.1 and 2.2 of this chapter.

To better understand how domestic companies are affected by the PIPL, Chinese company Didi's case study will be discussed in the following paragraph.

[220] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[221] Creemers, Rogier, Webster, Graham, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)

2.4.1 The case of DiDi Chuxing 滴滴出行's breach of the PIPL

DiDi Chuxing 滴滴出行 is one of the world's biggest mobile transportation platforms. Didi, formerly Didi Kuaidi 滴滴快递，was founded in 2012 by Cheng Wei 程维, who started his career working in Alibaba for eight years, first as a salesperson, then as deputy general manager. When Cheng Wei founded Didi, he intended it to be a smartphone app for people who wanted to immediately hail cabs.[222]

In February 2015, the two taxi-hailing companies Didi Dache 嘀嘀打车 and Kuaidi Dache 快递打车 were combined, in order to become the leader in China's rideshare market.

After its foundation, Didi started to provide a wider range of app-based mobility service options, e.g., Didi Premier, Didi Hitch, Didi Express. The services provided by Didi include e-bike sharing, taxi, car sharing, food delivery, car services and so on.

Besides the above-mentioned services that the company provides, Didi is also developing autonomous vehicle technology with a dedicated R&D subsidiary that completed two funding rounds raising US $825 billion (Caixin July 2021).

Among its achievements, Didi has changed the traditional taxi market pattern based on the characteristics of mobile Internet. It integrates online and offline to form an O2O closed loop, which reduces the empty driving rate and maximizes the saving of resources and time for both drivers and passengers.[223]

Globally, Didi has been expanding its partnership network with companies such as Lyft, Ola, Grab, 99, Taxify, and Careem, reaching more than 80% of the world's population and covering more than 1,000 cities. In 2018, Didi launched own-brand mobility services in Mexico and Australia, and formed a joint venture with SoftBank to offer a taxi-hailing service in Japan.

By continuously enhancing the user experience and creating social value, Didi aims to build an open, efficient, and sustainable transportation ecosystem and offer localized solutions to serve communities around the world.[224]

---

[222] DiDi. *Milestones*, https://www.didiglobal.com/about-special/milestone (Last Access: 04/04/2023)
[223] Li, Yixi, Wang, Meiyu, *Restore Customer Trust and Public Reputation: Case Study of Didi*, Proceedings of the 2022 7th International Conference on Financial Innovation and Economic Development (ICFIED 2022), 26/3/2022. Available at: https://www.atlantis-press.com/proceedings/icfied-22/125971978 (Last Access: 04/04/2023)
[224] Ibid.

Didi went public in an initial public offering (IPO) on June 30, 2021, when shares began trading on the New York Stock Exchange (NYSE) under the ticker symbol DIDI. The company sold 316.8 million American Depositary Shares (ADS), raising a total of $4.4 billion or $14 per share.[225]

The offering was larger than expected because the IPO was oversubscribed – Didi originally intended to sell 288 million shares – making it the largest listing by a Chinese company in the United States since Alibaba went public in 2014.[226]

Two days after Didi went public, China's top cybersecurity regulator – the Cyberspace Administration of China (CAC) – announced a cybersecurity review of the company.

On July 4, 2021 the company was ordered to suspend all new user registration for the duration of the review. In addition, Didi was removed from all app stores in China.

The CAC review's aim was to guard against national data security risk, to safeguard national security and public interest.

The suspension of its activities had a huge impact on the company, leading to a US $4.7 billion loss in revenue in the fourth quarter of 2021 and forcing it to cut spending and lay off staff in the beginning of 2022.[227]

Moreover, although the company aimed at listing in Hong Kong, this planning was blocked due to data security issues. As a consequence, the company's shares had a 44% decrease.

Due to such a devastating loss and after over 90 percent of shareholders voted in favor of the proposal, the company announced its delisting from the NYSE in May 2022.

On July 21, 2022, the CAC announced the results of the review: Didi violated the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law. Upon investigations, the company's illegal behavior is clear, the evidence conclusive, the circumstances grave, and the character despicable.[228] Therefore, such serious violations were severely punished.

---

[225] Wang, Echo, Sen, Anirban, Murdoch Scott, *China's Didi raises $4.4 bln in upsized U.S. IPO*, Reuters, 20/06/2021. Available at: https://www.reuters.com/business/chinas-didi-raises-4-billion-us-ipo-source-2021-06-29/ (Last Access: 03/04/2023)

[226] Ibid.

[227] Huld, Arendse, *How Did Didi Run Afoul of China's Cybersecurity Regulators? Understanding the US$1.2 Billion Fine*, China Briefing, 2/08/2022. Available at: https://www.china-briefing.com/news/didi-cyber-security-review-which-laws-did-didi-break/ (Last Access: 04/04/2023)

[228] Zhonghua Renmin Gongheguo Hulianwang Xinxi Bangongshi 中华人民共和国国家互联网信息办公室 (The Cyberspace Administration of China), *Guojia Hulianwang Xinxi Bangongshi Dui Didi Quanqiu Gufen Youxian Gongsi Yifa Zuochu Wangluo Anquan Shencha Xiangguan Xingzheng Chufa de Jueding* 国家互联网信息办公室对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定 (*The Cyberspace Administration of China has made a*

On July 7, the CAC imposed a fine of RMB 21.80 billion on Didi Global Co., Ltd., and RMB 26 million on Cheng Wei and Liu Qing, president of Didi.[229]

To sum up, the company was fined a total of RMB 8.026 billion, which correspond to US $1.2 billion.

To better explain which regulations Didi broke, the CAC published a Q&A – a set of answers to media questions – in which it clarifies how the review was conducted and what violations of laws and regulations Didi had.[230]

According to this Q&A, Didi had made sixteen violations covering eight types of activities:

1. Illegally collecting almost 12 million screenshots from users' mobile phone photo albums.
2. Collecting 8.3 billion pieces of information from users' clipboards and application lists in excess of the scope necessary to carry out operations.
3. Collecting 107 million pieces of facial recognition data, 53.5 million pieces of information on age groups, 16.3 million pieces on occupations, 1.4 million pieces of information on family relationships, and 153 million "home" and "company" addresses from passengers, in excess of the scope necessary to carry out operations.
4. Collecting 167 million pieces of information on the precise location (longitude and latitude) when passengers evaluated the driver services, both when the app was running in the background and when the mobile phone was connected to the Orange Video Recorder app (an app developed by Didi that enables dashcam recordings) in excess of the scope necessary to carry out operations.

---

decision on administrative punishment related to network security review against Didi Global Co., Ltd. Available at: http://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm (Last Access: (05/04/2023)

[229] Zhonghua Renmin Gongheguo Hulianwang Xinxi Bangongshi 中华人民共和国国家互联网信息办公室 (The Cyberspace Administration of China), *Guojia Hulianwang Xinxi Bangongshi Dui Didi Quanqiu Gufen Youxian Gongsi Yifa Zuochu Wangluo Anquan Shencha Xiangguan Xingzheng Chufa de Jueding* 国家互联网信息办公室对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定 (*The Cyberspace Administration of China has made a decision on administrative punishment related to network security review against Didi Global Co., Ltd*. Available at: http://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm (Last Access: (05/04/2023)

[230] For further information, please read: *Guojia Hulianwang Xinxi Bangongshi Youguan Fuzeren Jiu Dui Didi Quanqiu Gufen Youxian Gongsi Yifa Zuochu Wangluo Anquan Shencha Xiangguan Xingzheng Chufa de Jueding Da Jizhe Wen* 国家互联网信息办公室有关负责人就对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定答记者问 (*The relevant person in charge of the Cyberspace Administration of China answered reporters' questions on the decision to impose administrative penalties related to the cybersecurity review of Didi Global Co., Ltd. in accordance with the law*), 21/07/2022. Available at: http://www.cac.gov.cn/2022-07/21/c_1660021534364976.htm (Last Access: 05/04/2023)

5. Collecting 142,900 pieces of information on drivers' education and storing 57.8 million drivers' ID numbers in plain text in excess of the scope necessary to carry out operations.

6. Analyzing almost 54 billion pieces of information on passengers' travel intent information, 1.5 billion pieces of information on passengers' city of residence, and 304 million pieces of information of passengers' non-local business and travel information without clearly telling passengers.

7. Frequently requesting irrelevant phone permissions of passengers when using the ride-hailing service.

8. Failing to accurately and clearly explain the purpose for processing 19 types of personal information, including user device information.[231]

Moreover, the CAC stated that the company had also engaged in data processing activity that not only affected national security but also violated other laws and regulations. The CAC also added that Didi's illegal operations had exposed China's critical information infrastructure and data security to serious security risks. However, since these aspects were related to national security, the CAC did not reveal the details of such violations.

The above-mentioned violations occurred over the course of seven years, between 2015 and 2022 and showed that the company breached the three main regulations on data security and protection: the CSL (Cybersecurity Law), the DSL (Data Security Law) and the PIPL.

Given that the main focus of this paper is to investigate the main impacts the PIPL has on companies, only the specific part of the PIPL that were breached by Didi will be analyzed.

Among the violations listed above, items 2, 3, 4 and 5 can be considered as violations of the principle of minimum necessity, that is indicated in Article 6 of the Law. According to this article, data handlers are only allowed to collect and handle the scope of personal information to complete the express purpose of the processing and are not permitted to collect information that falls outside this scope.

Therefore, the information Didi collected was not required to fulfill the specific functions or services requested by the users.[232]

Another violation consists in processing and collecting users' personal information without clearly informing them about the purpose of the activity. This aspect breaches Article

[231] Huld, Arendse, *How Did Didi Run Afoul of China's Cybersecurity Regulators? Understanding the US$1.2 Billion Fine*, China Briefing, 2/08/2022. Available at: https://www.china-briefing.com/news/didi-cyber-security-review-which-laws-did-didi-break/ (Last Access: 04/04/2023)
[232] Ibid.

17 of the PIPL, according to which personal information handlers mist inform users in clear and understandable terms the purpose for handling their personal information. Moreover, in this case, the company did not pay enough attention to individuals' rights in personal information handling activities.

According to the violations listed above, Didi also breached the regulations on the handling of sensitive personal information. In fact, Didi did not comply with the PIPL in the handling of users' sensitive personal information, e.g., facial recognition data, information on users' age groups, occupations, family relationships, ID numbers.

For instance, item 1 of the above-mentioned violations, indicates that the company collected almost 12 million screenshots from users' mobile phones. As a consequence, although it is not specifically mentioned, these screenshots could have contained users' sensitive personal information. Moreover, in this case, the company's violation is even more serious as the information contained in these screenshots was not necessary to fulfill the processing activities.

Didi also violated informed consent rules, that are indicated in Article 14 of the PIPL. According to Article 14, the collection and processing of individuals' personal information are subject to the natural persons' consent. Without such consent, personal information handlers cannot collect or process personal information.

Therefore, when collecting users' personal information, Didi could collect and process such information only after the user is informed and agrees to the collection. If there is no consent from the user, it certainly constitutes an infringement.

When asked which was the main basis for the decision to impose administrative punishment on Didi, the CAC answered with five reasons that led to such a severe punishment.

First, on the character of the illegal activities, Didi failed to follow provisions of relevant laws and administrative regulations and the requirements of supervising departments in carrying out cybersecurity, data security, and personal information protection responsibilities. It disregarded national cybersecurity and data security, and posed serious risks and hidden dangers to national cybersecurity and data security.

When instructed by supervising departments to rectify matters, it nonetheless failed to conduct complete and thorough reforms.[233]

Second, on the duration of the illegal activities, the company's illegal activities began in June 2015 and lasted 7 years.

Third, on the harm from the illegal activities, Didi violated user privacy and damaged user personal information rights and interests by illegally collecting personal information, e.g., from within photo albums.

Fourth, on the scale of illegal handling of personal information, Didi illegally handled as many as 64.709 billion pieces of personal information. The scale of data was enormous, including many kinds of sensitive personal information.[234]

Fifth, on the circumstances of illegal handling of personal information, the company's illegal activities entail multiple apps and encompass different circumstances, such as excess collection of personal information and the collection of sensitive personal information.

As Arendse Huld – editor for China Briefing – says, the Didi case is the first major cybersecurity penalty to be levied by the CAC since several cyber and data security regulations have come into effect, and it reveals some of the ways in which companies may fall foul of regulators if they are careless in how they handle data or intentionally attempt to take advantage of users' information.[235]

As the CAC states in the Q&A, the penalties for the violations of Didi differ from general administrative penalties. Several elements can be considered as unusual: the seriousness of the violations and the size of the fine, as well as the attention this case has received from the media. However, all companies – especially SMEs – should keep in mind that the violations of regulations such as the PIPL could lead to serious consequences, including additional penalties, suspension of operations or public exposure. Therefore, even smaller penalties could pose a risk to enterprises which are not as big as Didi is.

---

[233] *Guojia Hulianwang Xinxi Bangongshi Youguan Fuzeren Jiu Dui Didi Quanqiu Gufen Youxian Gongsi Yifa Zuochu Wangluo Anquan Shencha Xiangguan Xingzheng Chufa de Jueding Da Jizhe Wen* 国家互联网信息办公室有关负责人就对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定答记者问 (*The relevant person in charge of the Cyberspace Administration of China answered reporters' questions on the decision to impose administrative penalties related to the cybersecurity review of Didi Global Co., Ltd. in accordance with the law*), 21/07/2022. Available at: http://www.cac.gov.cn/2022-07/21/c_1660021534364976.htm (Last Access: 05/04/2023)

[234] Ibid.

[235] Huld, Arendse, *How Did Didi Run Afoul of China's Cybersecurity Regulators? Understanding the US$1.2 Billion Fine*, China Briefing, 2/08/2022. Available at: https://www.china-briefing.com/news/didi-cyber-security-review-which-laws-did-didi-break/ (Last Access: 04/04/2023)

An additional aspect that should not be underestimated by companies is that new legislation and regulatory measures for data security have emerged and they make way more difficult for companies to hide from regulators and reduce the excuses for oversight.

The Didi case should be used by other companies, both domestic and foreign, as an example of how not do handle users' personal information, in order to stay in the good side of regulators. To do so, companies should train and educate IT personnel and operational

teams so that they are able to stay on top of the latest data protection requirements.

In addition, companies are also advised to consider protection mechanisms such as data encryption and implementing limited authorization to data access by employees, as well as conducting regular data protection impact assessments to ensure the security of the data and that no staff member unintentionally breaks any regulations.[236]

After a deep analysis on the impacts of PIPL on domestic companies and having provided the example of Didi Chuxing's illegal handling of personal information, it is necessary to focus on how this regulation affects foreign invested companies and multinational companies doing business in China.

2.5 The PIPL's impact on foreign invested enterprises

After its implementation, the PIPL has changed the way both foreign invested enterprises and multinational companies do business in China.

Before analyzing the PIPL's impact on foreign invested enterprises, it is important to mention how foreign direct investment (FDI) works in China.

In recent years, China has gradually become one of the countries with the largest levels of foreign direct investment (FDI).

Foreign direct investment has played a significant role in promoting Chinese economic development, and the FDI technology spillover effect is one of the core forces driving China towards reaching new growth milestones.[237]

[236] Huld, Arendse, *How Did Didi Run Afoul of China's Cybersecurity Regulators? Understanding the US$1.2 Billion Fine*, China Briefing, 2/08/2022. Available at: https://www.china-briefing.com/news/didi-cyber-security-review-which-laws-did-didi-break/ (Last Access: 04/04/2023)

[237] Zeng, Shihong, Ya Zhou, *Foreign Direct Investment's Impact on China's Economic Growth*, Technological Innovation and Pollution., International journal of environmental research and public health vol. 18,6 2839. 10 Mar. 2021, doi:10.3390/ijerph18062839

Foreign direct investments in China went through a big change and revolution after the New Foreign Investment Law (FIL) *waishang touzi fa* 外商投资法 came into effect on January 1, 2020. This new regulation's aim was to create a more open and transparent environment for foreign investments.

After it came into effect, the FIL replaced three existing laws: the Wholly foreign-owned enterprise Law of the People's Republic of China, the Sino-foreign equity joint venture enterprise Law of the People's Republic of China and the Sino-foreign cooperative joint venture enterprise Law of the People's Republic of China.

Those that must be compliant with the FIL include: foreign-invested enterprises, wholly foreign-owned enterprises, Sino-foreign joint ventures, investors in Hong Kong, Taiwan and Macau and individual foreign investors.

The FIL's scope of application is defined in Article 2 of the Law, which states that foreign investment refers to the investment activity directly or indirectly conducted by a foreign natural person, enterprise or other organization (the "foreign investors"), including the following circumstances:

1. A foreign investor establishes a foreign-funded enterprise within the territory of China, independently or jointly with any other investor;
2. A foreign investor acquires shares, equities, property shares or any other similar rights and interests of an enterprise within the territory of China;
3. A foreign investor makes investment to initiate a new project within the territory of China, independently or jointly with any other investor; and
4. A foreign investor makes investment in any other way stipulated by laws, administrative regulations or provisions of the State Council.[238]

Furthermore, Article 2 defines a foreign-funded enterprise as

> an enterprise that is incorporated under the Chinese laws within the territory of China and is wholly or partly invested by a foreign investor.[239]

[238] *Foreign Investment Law of the People's Republic of China*, National Development and Reform Commission (NDRC) People's Republic of China, 24/02/2021. Available at: https://en.ndrc.gov.cn/policies/202105/t20210527_1281403.html
[239] Ibid.

Moreover, the nature of foreign-invested enterprises themselves determines that they are a more globalized class of enterprises, and it is not uncommon for data to be stored on servers, affiliates or suppliers outside of the country.[240]

This definition included in Article 2 of the FIL shows how the FIEs have the same obligations as domestic companies as they are incorporated under the Chinese law. However, they also keep in touch and share information with their offshore parent entity, as a consequence, when they transfer and manage Chinese citizens' personal information outside the borders of the PRC, they are subjects to additional obligations which are stated in Chapter III of the PIPL.

Therefore, as one of the most restrictive data privacy laws in the world, PIPL creates significant hurdles to the business operation of foreign invested enterprises (FIEs) in China, especially in connection with internal investigations.[241]

2.6 The PIPL's impact on multinational companies

In general, multinational companies doing business in China are hugely affected by the new PIPL, as in the majority of cases personal information (e.g., employees' data or customers' data) are shared between headquarters and subsidiaries.

When focusing on the impact on multinational companies, it is necessary to underline that, according to Article 3 of the PIPL, the law applies to overseas companies under three circumstances:

1. Where the purpose is to provide products or services to natural persons inside the borders;
2. Where analyzing or assessing activities of natural persons inside the borders;
3. Other circumstances provided in laws or administrative regulations.[242]

---

[240] Zhong, Xin 钟新, *Waizi Qiye Hegui Guanli Shuju Anquan* 外资企业合规管理之数据安全 *(Data Security for Compliance Management of Foreign-funded Enterprises)*, Guohao Lushi Shiwu Suo 国浩律师事务所 (Grandall Law Firm), 28/07/2021. Available at: https://www.grandall.com.cn/ghsd/info_17.aspx?itemid=23984 (Last Access 08/04/2023)

[241] Li, Yiqiang, *Challenges Under New Personal Information Protection Regime in China*, Faegre Drinker, 25/8/2021. Available at: https://www.faegredrinker.com/en/insights/publications/2021/8/challenges-under-new-personal-information-protection-regime-in-china (Last Access: 06/05/2023)

[242] Creemers, Rogier, Webster, Graham, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)

According to Li Yiqiang, the first two circumstances may apply to offshore e-commerce business targeting Chinese domestic consumers. However, the application of the second circumstance is much broader and could extend to employment, education and even business due diligence managed by an offshore entity.[243]

As it was stated, in the majority of cases multinational companies transfer important information between headquarters and subsidiaries. Therefore, the first aspect that foreign companies operating in China must be compliant with is cross-border data transfer. Such aspect is deeply explained in Chapter III of the PIPL and has a huge impact on how foreign companies do business in China.

During a roundtable at the International Association of Privacy Professionals[244], Yan Luo – Partner at Washington-based law firm Covington & Burling – said that multinational companies will probably need to start from scratch and establish an internal program to manage cross-border data transfers.

The provisions on cross-border data transfer and which measures must be adopted by companies in order to be compliant with the PIPL will be investigated in chapter III of this paper.

Although the impact of cross-border data transfer provisions could seem to be the most prominent one, there are also other aspects that should not be underestimated.

First, it is necessary to focus on the main impacts the PIPL has on foreign companies: the cost impact and the IT impact.

Concerning the cost impact, data localization and IT investments may increase compliance costs. Lester Ross – Partner-in-charge of the Beijing office at U.S. law firm WilmerHale – says that the pressure to store personal information within China will raise costs. He also explains that this may include the need to establish a separate PI storage operation or otherwise handle PI-related matters within China.[245]

Concerning the IT impact, the data localization requirement of the PIPL has a big impact on the IT infrastructure of a company.

---

[243] Li, Yiqiang, *Challenges Under New Personal Information Protection Regime in China*, Faegre Drinker, 25/8/2021. Available at: https://www.faegredrinker.com/en/insights/publications/2021/8/challenges-under-new-personal-information-protection-regime-in-china (Last Access: 06/05/2023)

[244] Available at: https://www.linkedin.com/video/live/urn:li:ugcPost:6841007885883871232/

[245] Ghosh, Soumik, *How China's Information Protection Law Affects Businesses*, Bankinfosecurity, 09/09,2021. Available at: https://www.bankinfosecurity.asia/how-chinas-information-protection-law-affects-businesses-a-17498 (Last Access: 17/03/2023)

Experts say that meeting compliance guidelines for software development kits can be tricky. For instance, Jacobo Esquenazi Franco – global privacy strategist and DPO for European Union at technology company HP – says that that there is data being collected and, in some cases, transferred where companies do not have control. The application might be collecting and transferring data for another controller without consent nor a legal basis, and that can lead to violations.[246]

Furthermore, when designing the IT infrastructure, companies should keep in mind that even if data is stored in China in standalone IT infrastructure, it would still be treated as cross-border transfer if a user outside of China has remote access to the data.

A solution suggested by Xiaomi head of security and privacy compliance Kevin Song is that companies should conduct careful inspection of third-party SDKs (software development kits) and design a privacy interface. By doing so, companies will be able to protect user rights and make the data life cycle transparent.

Additionally, Lester Ross indicated three principles that IT leaders of multinationals should consider: seeking individuals' consent to collect and process personal information, anonymizing before exporting and drawing contracts to govern relationships with PI custodians and processors, security consultants and overseas transferees.[247]

Once that the two major impacts on foreign companies have been analyzed, it is important to focus on the measures foreign companies should adopt.

When dealing with personal information protection, companies have to understand the practices regarding personal information protection inside the organization. To do so, they need to answer to four questions:

a) Who collects the data, in which way, from whom, and for what purpose?

b) Which system is used to save personal data and in which format? Where is the physical location of the system?

c) Who has access to the data and for what purpose?

d) Is the data being shared with a third party and for what purpose, if any?[248]

---

[246] Ghosh, Soumik, *How China's Information Protection Law Affects Businesses*, Bankinfosecurity, 09/09,2021. Available at: https://www.bankinfosecurity.asia/how-chinas-information-protection-law-affects-businesses-a-17498 (Last Access: 17/03/2023)

[247] Ibid.

[248] Zhang, Thomas, *PIPL China: Suggestions for Technical Compliance with Personal Information Protection Law*, China Briefing, 25/10/2021. Available at: https://www.china-briefing.com/news/pipl-china-suggestions-on-technical-measures-for-compliance/ (Last Access: 11/04/2023)

Answers to these questions can be found in data mapping, which is:

> the process of matching fields from one database to another. It's the first step to facilitate data migration, data integration, and other data management tasks.[249]

Moreover, a key solution for companies is to have a personal data protection team which identifies the flow of personal information within the organization and between external parties. A way to do so, is to carry out a Data Protection Impact Assessment (DPIA), to identify risks to personal data and analyze how systems collect, share, use and store personal data.

Another way to manage and reduce risks posed to personal information protection is to use de-identification technology, that is, anonymizing the personal information that a company handles. However, through this technology some insights are lost. As a consequence, striking a balance between the usability of personal information and the protection of said information is therefore a typical challenge that companies face.[250]

Among the other adoptable measures, companies should hire a privacy team with qualified privacy expertise which is composed by both legal and technology experts to deal with compliance risks.

Lastly, companies should emphasize privacy awareness training to make sure all staff are aware of the importance of personal information protection to the business, clients, other third parties and themselves.[251]

In conclusion, we can notice how foreign companies operating in China are facing a lot of challenges created by the data sovereignty provisions of the PIPL, especially when facing legal reporting obligations to their home countries. In fact, as Li Yiqiang says, they will probably need to make a choice to deal with the conflicts of legal obligations imposed by China and their home countries after evaluating the risks of available options.[252]

The new legal environment is so challenging that some companies decided to leave China. For instance, when the PIPL came into effect, Yahoo! announced it would cease operating in China because of its "increasingly challenging business and legal environment".

---

[249] *What is Data Mapping*?, Talend. Available at: https://www.talend.com/resources/data-mapping/
[250] Zhang, Thomas, *PIPL China: Suggestions for Technical Compliance with Personal Information Protection Law*, China Briefing, 25/10/2021. Available at: https://www.china-briefing.com/news/pipl-china-suggestions-on-technical-measures-for-compliance/ (Last Access: 11/04/2023)
[251] Ibid.
[252] Li, Yiqiang, *Challenges Under New Personal Information Protection Regime in China*, Faegre Drinker, 25/8/2021. Available at: https://www.faegredrinker.com/en/insights/publications/2021/8/challenges-under-new-personal-information-protection-regime-in-china (Last Access: 26/03/2023)

In addition, Microsoft-owned LinkedIn announced that LinkedIn would be shutting down in China due to China's "significantly more challenging operating environment and greater compliance requirements."[253]

However, those foreign companies which still have operations in China will first need to be prepared to develop a compliance system and then adopt the measures explained above.

2.7 The PIPL's implications on marketing, online advertising and human resources management

As we have seen in the previous paragraphs, China's Personal Information Protection Law constitutes a big challenge for domestic companies as well as foreign companies operating in China. This new regulation forces all companies to make changes in the way they do business: such changes can affect different areas such as the human resources management, the marketing area, online advertising, and so on. In some cases, because of the implications on this new law, companies could also have to make changes in their whole business models.

In this paragraph the impact of China's PIPL on different areas of business will be investigated, with a particular focus on the areas of digital marketing and online advertising. The impact on human resource management will be analyzed in Chapter III of this paper.

2.7.1 The impact on digital marketing

On January 16, 2022 the Chinese magazine Qiushi 求是 published an article written by the People's Republic of China President Xi Jinping 习近平.

This article – entitled "Continuously Strengthening, Optimizing and Expanding China's Digital Economy" – stressed that in recent years the digital economy has developed at rapid

[253] Kipfer, Arlo, *China's New Personal Information Protection Law Forced Out Yahoo and Linkedin: Will YOU Be Next*, China Law Blow, Harris Bricken, 11/09/2021. Available at: https://harrisbricken.com/chinalawblog/chinas-new-personal-information-protection-law-forced-out-yahoo-and-linkedin-will-you-be-next/ (Last Access: 11/04/2023)

pace and is becoming a key force in reorganizing global factor resources, reshaping the global economic structure and changing the global competitive landscape.[254]

Since digital marketing industry is an essential part of the digital economy, it plays a vital role in its continuous development.

In the 2021 China Digital Marketing Industry Research, digital marketing was defined as:

> the practice of promoting products and services using digital communication channels to communicate with consumers in a timely, relevant, customized and cost-effective manner.[255]

In addition, digital marketing can also be defined as the process of marketing services through big data operation and analysis, which focuses on mining customer needs and satisfying them.

Therefore, the access to data and the analysis of data are crucial steps to understand customers' needs, to provide them personalized recommendations, and to enhance customers' satisfaction.

After its implementation in November 1, 2021, China's PIPL opened a new chapter for all areas of business, and digital marketing is no exception.

Because of the PIPL's implications, marketers will face different challenges. Among them, four will be investigated in this paper.

First, the difficulty in data acquisition has increased. According to Article 6 of the PIPL, the collection of personal information should be limited to the minimum scope for achieving the handling purpose and excessive collection of personal information should not be allowed. This reduces the scope of legal collection of users' personal information by companies in their interactions with consumers, and poses a great obstacle to companies relying on big data operations and analysis to make marketing decisions.[256]

---

[254] Xu, Manjing, Wang, Dongxu, Peng, Beisen, 许蔓菁, 王东旭, 彭焙森, *Geren Xinxi Baohufa Shishi Xia de Shuzi Yingxiao Fazhan Tantao*《个人信息保护法》实施下的数字营销发展探讨 (*Discussion on the development of digital marketing under the implementation of "Personal Information Protection Law"*), Xiandai Shangye 现代商业 (Modern Business Magazine) 2023, No.663(02): 32-35. Available at: https://www.xdsyzzs.com/zixun/7920.html

[255] Aimei Zixun (iiMedia)艾媒咨询，*2021 Nian Zhongguo Shuzihua Yingxiao Hangye Yanjiu Baogao* 2021年中国数字化营销行业研究报告 (*China Digital Marketing Industry Research 2021 Report*), 18/01/2022. Available at: https://www.iimedia.cn/c400/83281.html (Last Access: 14/04/2023)

[256] Xu, Manjing, Wang, Dongxu, Peng, Beisen, 许蔓菁, 王东旭, 彭焙森, *Geren Xinxi Baohufa Shishi Xia de Shuzi Yingxiao Fazhan Tantao*《个人信息保护法》实施下的数字营销发展探讨 (*Discussion on the development of digital marketing under the implementation of "Personal Information Protection Law"*), Xiandai Shangye 现代商业 (Modern Business Magazine) 2023, No.663(02): 32-35. Available at: https://www.xdsyzzs.com/zixun/7920.html

Data acquisition is a key aspect of marketing activities in all companies, but is particularly relevant for large-scale Internet platforms, e.g., WeChat and TikTok.

Social media platforms are *two-sided markets*[257]: they are intermediaries who provide digital services to users, but they also monetize their data by selling services based on

those data to other customers, with advertisers being the most important sources of revenue.[258]

Social media platforms commonly collect users' data in three ways:

a) through their own platform software;

b) from third-party advertisers;

c) by storing user-generated data contributed for either commercial or non-commercial purposes.[259]

If we analyze the new regulations on data security, the Chinese approach is impact-orientated, that is, it allows data subjects to seek redress only when harm is of significant social impact.[260] Therefore, this approach emphasizes the liability of service providers and the obligation to prevent data breaches.

As we have already seen in paragraph 2.1 of this chapter, according to Article 58 of the PIPL, large-scale platforms have additional obligations, as personal information handlers that provide important Internet platform services shall fulfill four obligations:

1. Establish and complete personal information protection compliance systems and structures according to State regulations, and establish an independent body composed mainly of outside members to supervise personal information protection circumstances;

2. Abide by the principles of openness, fairness, and justice; formulate platform rules; and clarify the standards for intra-platform product or service providers' handling of personal information and their personal information protection duties;

3. Stop providing services to product or service providers on the platform that seriously violate laws or administrative regulations in handling personal information;

[257] Rochet, Jean-Charles, Tirole, Jean, *Platform Competition in Two-Sided Markets,* Journal of the European Economic Association, 1(1), 1990 June 2003, 990–1029. https://doi.org/10.1162/154247603322493212
[258] Xue, Janet Hui, *Delegitimising Data Subjects' Economic Interests During Automatic Propertisation of Their Data: A Comparative Study of Data Protection on Social Media Platforms in the UK and China*, Global Media and China, 7(2), 151–168, 2022. https://doi.org/10.1177/20594364211060874
[259] Ibid.
[260] Ibid.

4. Regularly release personal information protection social responsibility reports, and accept society's supervision.[261]

These obligations make the accomplishment of marketing activities way more challenging for large-scale Internet platforms.

The second consequence is a limitation in the marketing model's personalization. As it has already been mentioned, digital marketing is the use of a large amount of accurate data for personalized marketing. However, according to Article 24 of the PIPL, users have the right to refuse being automatically targeted in commercial sales based on their personal characteristics. Moreover, this Article also states that automated decision-making must be transparent and fair and that personal information handlers shall not impose unreasonable differential treatment on individuals in terms of transaction prices and other trading conditions.

These two provisions have two consequences: the first one is that companies can no longer treat users differently according to their consumption habits, different terminals, preferences, etc. The second one is that companies must provide customers with a convenient way to refuse personalized content, and not to refuse to provide the service of product to the user because he or she refuses personalized recommendations.

Therefore, although this article is very convenient to customers as they can exercise their right to refuse personalized content push, it also limits the possibility for company to provide personalized services and recommendations. Thus, it hinders the progress of digital marketing.[262]

The third consequence of the PIPL on digital marketing is platform data desensitization and private domain traffic changes.

Private domain traffic marketing can be defined as:

---

[261] Creemers, Rogier, Webster, Graham, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)

[262] Xu, Manjing, Wang, Dongxu, Peng, Beisen, 许蔓菁, 王东旭, 彭焙森, *Geren Xinxi Baohufa Shishi Xia de Shuzi Yingxiao Fazhan Tantao*《个人信息保护法》实施下的数字营销发展探讨 (*Discussion on the development of digital marketing under the implementation of "Personal Information Protection Law")*, Xiandai Shangye 现代商业 (Modern Business Magazine) 2023, No.663(02): 32-35. Available at: https://www.xdsyzzs.com/zixun/7920.html

> the method whereby a brand's communication with its customers is "funneled" into private channels (i.e., "private domains *siyu* 私域"), where it has complete control over how and when it wants to communicate with this audience.[263]

In other words, private domains are the opposite of public domains *gongyu* 公域 that are instead traffic sources not controlled by brands.

The purpose of using private domains for companies is to make sure that customers keep remembering their products or services even after they buy them or after leaving the companies' websites. Therefore, private domains are a tool that can be used to make sure that the company keeps being fresh on the users' minds.

The PIPL not only makes it more difficult to collect personal information, but also increases the responsibility of platforms, requiring e-commerce platforms to *desensitize* data, which means that the data merchants get from the platform will be encrypted, which may have an impact on the original marketing strategy[264]

As a consequence, this aspect does not reduce the use of private traffic, but it increases it. In fact, given that companies can no longer rely on the data source of the platform, they must establish their own exclusive data channels to enhance user stickiness.[265]

The fourth consequence is the increased scrutiny of cross-border businesses. Chapter III of the PIPL provides provisions on cross-border data management and sets out the procedures for cross-border data flow. Companies must meet the conditions indicated in Article 38 in order to transfer personal information abroad, and this is particularly relevant for those multinational companies that have subsidiaries in China or those Chinese enterprises that are listed abroad.

After having analyzed the main impact that the PIPL has on digital marketing, companies must figure out how to develop digital marketing in compliance with the new regulation.

---

[263] *How to Leverage Private Domain Traffic in China*, The Egg. Available at: https://www.theegg.com/social/china/how-to-leverage-private-domain-traffic/#:~:text=What%20is%20private%20domain%20traffic,to%20communicate%20with%20this%20audience (Last Access 16/04/2023)

[264] Xu, Manjing, Wang, Dongxu, Peng, Beisen, 许蔓菁, 王东旭, 彭焙森, *Geren Xinxi Baohufa Shishi Xia de Shuzi Yingxiao Fazhan Tantao*《个人信息保护法》实施下的数字营销发展探讨 (*Discussion on the development of digital marketing under the implementation of "Personal Information Protection Law")*, Xiandai Shangye 现代商业 (Modern Business Magazine) 2023, No.663(02): 32-35. Available at: https://www.xdsyzzs.com/zixun/7920.html

[265] Ibid.

First, companies should study the relevant legal provisions on data security and, therefore, establish a legal awareness. Such awareness should be gained by all members of a company's staff, and not just by personnel dealing with legal affairs.

Second, companies should promote a high-quality development of digital marketing. This high-quality can be achieved in three ways: the first one is to change the business philosophy. It means that although the difficulty in obtaining individuals' data has increased, companies should optimize the way they collect data and value customer experience. By doing so, a part of users will probably not refuse personalized recommendations. The second is to enhance customer stickiness and establish a closer relationship with users by paying more attention to private domain traffic. The third is innovation. Companies should seek ways to innovate within a reasonable and legal scope.

Last aspect that companies can do to develop digital marketing under the PIPL is to strengthen internal management. This requires companies to form a corresponding corporate culture, carried out to the hearts of every company employee. Enterprises should improve their compliance management capabilities in daily management, instill awareness of data security risk prevention to all employees, and also adhere to the principle of consistency to ensure that relevant sensitive information and confidential data are handled consistently.[266]

Moreover, in order to strengthen internal management, companies should focus on two aspects: training and supervision.

For what concerns training, companies should train relevant personnel, clarify work procedures, legal boundaries and reasonable methods for collecting users' information. Regarding supervision, companies should supervise daily data collection and processing and punish staff who violate relevant systems in accordance with regulations.

In conclusion, we can notice how the PIPL's implementation not only has had a great impact on digital marketing, as it has limited the amount of users' data that companies collect, and has changed the way companies collect it, but it has also forced and still forces companies to seek new ways to innovate their business.

[266] Xu, Manjing, Wang, Dongxu, Peng, Beisen, 许蔓菁, 王东旭, 彭焙森, *Geren Xinxi Baohufa Shishi Xia de Shuzi Yingxiao Fazhan Tantao*《个人信息保护法》实施下的数字营销发展探讨 (*Discussion on the development of digital marketing under the implementation of "Personal Information Protection Law")*, Xiandai Shangye 现代商业 (Modern Business Magazine) 2023, No.663(02): 32-35. Available at: https://www.xdsyzzs.com/zixun/7920.html

2.7.2 The impact on online advertising industry

The impact of privacy laws on the value created in the online advertising market is likely to be substantial because firms operating in this market heavily rely on personal data processing to provide users with personalized offerings.[267]

Kumar and Rajan define value for an actor as:

> the net accrued benefits (tangible and intangible) over the associated costs that firms and individuals realize in a commercial exchange process.[268]

Privacy laws affect value in two ways: first, they affect firms as they need to create value for multiple stakeholders; second, they affect users as they need to know how their privacy is protected by the law and they also should know the consequences of their choices (for instance, if they decide to protect their privacy, they will receive less relevant advertisements).

Since its implementation, the PIPL has had a huge impact on online advertising industry. In fact, Feng Qingqing 冯清清 – a senior partner at Guangyue Law Firm – said that for the digital advertising industry, the prominent impact of the PIPL is concentrated in the front end, that is, the collection and use of personal information.[269]

Therefore, regulators focus on rectifying the collection of personal information beyond the scope in the course of law enforcement, and require the principle of minimum necessity to be followed.

To better analyze and understand the online advertising market, it is necessary to focus on its main actors.

There are three primary actors in the online advertising industry: advertisers, whose goal is to draw users' attention and interest to the advertisers' offerings; publishers who monetize

---

[267] Skiera, Bernd, Miller, Klaus, Jin, Yuxi, Kraft, Lennart, Laub, Rene, Schmitt, Julia, *The impact of the general data protection regulation (GDPR) on the online advertising market*, Self-Publishing, 2022.
[268] Kumar, V., Bharath Rajan, *What's in It for Me? The Creation and Destruction of Value for Firms from Stakeholders*, Journal of Creating Value 3.2 (2017): 142-56.
[269] *Jingzhun Yingxiao Moshi Shoucuo Xin Jishu Qianghua Yinsi Baohu Hou ge Baohu Shidai Shuzi Guanggao Hangye Zhe Ji Haishi Biange* 精准营销模式受挫，新技术强化隐私保护，后个保法时代数字广告行业折戟还是变革？ (*The precision marketing model has suffered setbacks, and new technologies have strengthened privacy protection. Will the digital advertising industry collapse or change in the post-law protection era?),* Shiji Jingji Baodao 21 世纪经济报道 21 (21st Century Business Herald), 7/11/2022. Available at: https://m.21jingji.com/article/20221107/herald/aa25db972571ed7c9a557332e02463ec_zaker.html (Last Access: 20/04/2023)

their services by selling ad spaces to advertisers; users who are interested in the publishers' offerings and in the ads displayed.[270]

As Skiera et al. have identified, among these three actors, three kinds of exchanges occur.

The first exchange is between users and publishers. Publishers provide users free content in exchange for processing their personal data. Moreover, they provide contact between users and advertisers.

The second exchange is between advertisers and publishers. Advertisers pay publishers, whose aim is to contact users. If the users' personal data received are useful to improve the ad effectiveness, the publishers will be paid more.

The last exchange is between users and advertisers. After seeing the ads targeted and personalized for the users, the latter can decide to purchase the advertisers' offerings.

The analysis of these exchanges shows the crucial role of collecting and processing data in online advertising industry, as tracking and profiling have a vital importance in each exchange.

Given that the China's PIPL provides users with rights and impose obligation on personal information handlers (in this case publishers and advertisers) to limit data processing, advertisers, publishers and users are the main actors affected by the PIPL in the online advertising market.

Concerning the privacy laws' impact on firms, a study conducted by Bernd Skiera and Yuxi Jin has shown how the impacts depend on the firm's size and category. For instance, Schmitt et al. found negative effects on publishers' user contacts throughout the observation period for some industries (e.g., Arts and Entertainment) and positive effects for some others (e.g., Business and Consumer Services), whereas positive effects occur in the short term and negative effects in the long term for categories such as e-commerce and shopping.[271]

Although the above-mentioned study was based on a comparison between EU's GDPR, California Consumer Privacy Act (CCPA) and the PIPL, it can still be used for the purpose of this paper, that is to investigate how the online advertising industry is affected by the China's PIPL.

Regarding the PIPL's impact on users, it depends on two factors: users' preferences for personalization and users' sensitivity to privacy infringement.

---

[270] Jin, Yuxin, Skiera, Bernd, *How Do Privacy Laws Impact the Value for Advertisers, Publishers and Users in the Online Advertising Market? A Comparison of the EU, US and China*, Journal of Creating Value, 8(2), 306–327, 2022. https://doi.org/10.1177/23949643221117676

[271] Ibid.

A study on the former aspect shows that for those users who used to be in favor of personalized offerings, utility for personalization decreases, as the PIPL has made personalization more costly with the opt-in consent banner. On the other hand, for those users who do not obtain utility from personalization, their utility from personalized recommendations is not affected by the consent banners.

Meanwhile, for what concerns users' sensitivity to privacy infringement, users who are more sensitive to a privacy loss benefit more from the protection provided by the PIPL.

In general, the PIPL's impacts on online advertising industry can be divided into two categories: positive and negative.

The negative effects come from three sources:

a) Users of the consent management tools making choices to opt-out from data processing;

b) Firms making choices to work with fewer firms to avoid legal risks;

c) Legal requirements imposing compliance cost to users and firms.[272]

The first two sources lead to a reduction in the number of user contacts and user data that are useful for tracking and profiling. This reduction of users' data lowers firms' targeting accuracy and, therefore, decreases publishers and advertisers' revenue from their offerings.

Because of the third source, among the costs that firms bear, there is the cost of creating technical and legal infrastructures. Moreover, firms also run the risk of violating the law.

Meanwhile, users' costs include the decision cost to take control of their data.

The positive impacts also originate from three sources:

a) users gaining utility from privacy protection;

b) industry leaders such as Facebook and Google benefiting from the increased market concentration, as they own a larger share of a smaller pie;

c) zero-sum value transfer from advertisers to publishers: the decrease of publisher ad revenue equals the decrease of advertiser ad spending, that is, lower cost and higher value for advertisers.[273]

To sum up, this study shows how the changes in value are the largest in absolute terms for publishers, followed by users and advertisers.

---

[272] Jin, Yuxin, Skiera, Bernd, *How Do Privacy Laws Impact the Value for Advertisers, Publishers and Users in the Online Advertising Market? A Comparison of the EU, US and China*, Journal of Creating Value, 8(2), 306–327, 2022. https://doi.org/10.1177/23949643221117676

[273] Jin, Yuxin, Skiera, Bernd, *How Do Privacy Laws Impact the Value for Advertisers, Publishers and Users in the Online Advertising Market? A Comparison of the EU, US and China*, Journal of Creating Value, 8(2), 306–327, 2022. https://doi.org/10.1177/23949643221117676

Publishers are the ones who are the most affected negatively because if user utility from consuming publisher offerings decreases, value decreases. Therefore, due to reduced ad revenue, publishers cannot afford the cost of providing high-quality offerings, causing a decrease in the quality of the publishers' offerings.

However, it is important to understand how companies operating in the online advertising industry really comply with the PIPL regulation.

In order to be compliant with Article 24 of the PIPL, all companies have updated their privacy clauses. However, according to Song Xing - a senior practitioner of data-based Internet marketing – in China personalized ads are currently most always turned on by default. Moreover, he found that the steps to turn off personalized advertising are usually very cumbersome, making very difficult for users to turn off personalized advertising options.[274]

In addition, according to Sue Yang – head of privacy in Asia Pacific – in the year since the PIPL landed, most companies in the industry have successively cleaned up previously obtained data, which is data that has not been authorized by users or is incomplete. This cleanup process requires time, resources, and monetary costs.[275]

In general, we notice how after the PIPL came into effect, the online advertising industry is facing different challenges, but is also going through a phase of big innovation that is going to change the way users' data is collected, processed and how personalized advertisements are provided.

Among the changes that will occur, Liao Huaixue 廖怀学 – a lawyer at Tahota Law Firm *taihe tai lushi shiwu suo lushi* 泰和泰律师事务所律师 – said that in the future development process, it is necessary to pay attention to two balances: the first one is the balance between

[274] Xu, Mingjiao 徐明皎, *Geren Xinxi Quanmian Baohu Shidai Shuzihua Yingxiao Yinglai Biange* 个人信息全面保护时代 数字化营销迎来变革 (*In the era of comprehensive protection of personal information, digital marketing ushered in changes*), Fazhiwang 法治网 (Legal daily), 7/12/2021. Available at: http://www.legaldaily.com.cn/zt/content/2021-12/07/content_8640081.htm (Last Access: 21/04/2023)

[275] *Jingzhun Yingxiao Moshi Shoucuo Xin Jishu Qianghua Yinsi Baohu Hou ge Baohu Shidai Shuzi Guanggao Hangye Zhe Ji Haishi Biange* 精准营销模式受挫，新技术强化隐私保护，后个保法时代数字广告行业折戟还是变革？ (*The precision marketing model has suffered setbacks, and new technologies have strengthened privacy protection. Will the digital advertising industry collapse or change in the post-law protection era?),* 21 Shiji Jingji Baodao 21 世纪经济报道 (21st Century Business Herald), 7/11/2022. Available at: https://m.21jingji.com/article/20221107/herald/aa25db972571ed7c9a557332e02463ec_zaker.html (Last Access: 21/04/2023)

commercial interests and user experience, so as not to interfere with users and reasonably develop the industry; the second is the balance between the needs of the advertising industry and the security of personal information.[276]

In conclusion, it is possible to state that the PIPL is both a restriction and a threshold, as companies need to find a new balance between user privacy protection and industry interests through the exploration of new technologies for privacy protection, new models for business development, and new data compliance systems.

As Sue Yang believes, the legislative purpose of the PIPL is not to restrict the development of the industry, but to promote it. Furthermore, she said that the PIPL has eliminated the gray area of digital advertising data compliance. After this new Law's implementation, the industry has entered a new stage of data collection and use, the relevant provisions on consumer authorization are clearer, and the data compliance standards between different enterprises have been clear and unified. Moreover, she believes that in the future the industry will be able to accurately reach consumers on the basis of legal compliance while focusing on consumer experience.[277]

Therefore, we notice how the PIPL, on the one hand has added new restrictions in personal information processing and, therefore, forced companies to face big challenges in order to be compliant with the law; on the other one, it has also transformed the online advertising industry, as it has forced companies to focus on innovation.[278]

After a deep analysis of how the China's PIPL affects different areas of business, with a particular focus on marketing and online advertising industry, the next chapter will focus on companies' human resource management and how employees' personal information is collected, processed and, if necessary, transferred.

---

[276] *Jingzhun Yingxiao Moshi Shoucuo Xin Jishu Qianghua Yinsi Baohu Hou ge Baohu Shidai Shuzi Guanggao Hangye Zhe Ji Haishi Biange* 精准营销模式受挫，新技术强化隐私保护，后个保法时代数字广告行业折戟还是变革？ (*The precision marketing model has suffered setbacks, and new technologies have strengthened privacy protection. Will the digital advertising industry collapse or change in the post-law protection era?),* 21 Shiji Jingji Baodao 21 世纪经济报道 (21st Century Business Herald), 7/11/2022. Available at: https://m.21jingji.com/article/20221107/herald/aa25db972571ed7c9a557332e02463ec_zaker.html (Last Access: 21/04/2023)

[277] Ibid.

[278] For more details, please read this article: *Geren Xinxi Baohufa Shishi Hou HulianWang Guanggao de Weilai Zai Nali?* 个人信息保护法实施后，互联网广告的未来在哪里？ (*How is the future of Internet advertising after the implementation of the Personal Information Protection Law?)* https://new.qq.com/rain/a/20211102A0A7O000 (Last Access: 21/04/2023)

Chapter 3. PIPL's impacts on Human Resources Management

As it has been noted in the previous chapter, China's Personal Information Protection Law has a huge impact on different areas of business.

In particular, human resource management, which includes the recruitment and employment of individuals, is deeply affected by this new regulation, as it is an area of business in which the collection of personal information is essential.

Despite the size or the place where it is located, in every company, the HR department handles a large amount of personal data about their former, current and potential employees. Therefore, for any company, employees' personal information constitutes an extremely valuable resource which must be protected.

The mishandling of employees' information or the incapability to protect it could lead to serious consequences for both the employees and the reputation of the company. In order to increase and implement employees' data protection, data privacy regulations from all around the world have laws set in place which obligate employers to protect the employees' personal data and prevent an incident of a breach occurring[279], and the PIPL is no exception.

Given the crucial role that the handling of personal information has in the human resource management, all companies must ensure to be compliant with the PIPL when processing employees' personal data.

3.1 Employees' Personal Information Protection in China

In order to deeply understand employees' personal information protection in China, it is necessary to mention some key points of Chinese labor legal system.

The 1994 Labor Law and the 2008 Labor Contract Law are the two primary sources of employment law in China.

The first wave of modern labor law reform appeared in 1994 with the passage of the Labor Law, as a response to large-scale protests denouncing workers' exploitation[280].

Since the promulgation of the Labor Law of the People's Republic of China *zhonghua renmin gongheguo laodongfa* 中华人民共和国劳动法 in 1994, great achievements have

[279] Privacy Research Team, *The HR Guide to Employee Data Protection*, Securiti, 26/08/2022. Available at: https://securiti.ai/blog/hr-employee-data-protection/ (Last Access: 28/05/2023)
[280] Garcia, Monique, *China's Labor Law Evolution: Towards A New Frontier*, ILSA Journal of Int'l & Comparative Law, Vol. 16:1, p. 237.

been made in the construction of China's labor legal system, which has played an important role in protecting the basic rights of workers, maintaining stable and harmonious labor relations, and promoting the development of market economy.[281]

Although China's Labor Law's main purpose was to protect workers from employers' exploitation, it was not a big success. Such failure was due to two main reasons: first, the laws varied from district to district, as the local governments were the primary source of implementation of the laws; second, the Labor Law was regularly breached by employers, as they perceived it as a voluntary and non-binding regulation.

Therefore, the 1994 Labor Law was viewed as a non-binding voluntary proposal by domestic and foreign investment enterprises and because there were no enforcement mechanisms in place, the provisions were neither respected nor enforced.[282]

This situation started to change in 2007, following massive labor protests, which were raised after Chinese press reports revealed that in the Shanxi 山西 and Henan 河南 provinces, the police had freed almost 600 workers (many of them children) who were held as slave laborers.

As a response to these protests, the new Labor Contract Law *zhonghua renmin gonghehuo laodong hetong fa* 中华人民共和国劳动合同法 was adopted on June 29, 2007 and became effective on January 1, 2008.

Article 1 of the Labor Contract Law states the purposes of the law, which are:

> the purposes of improving the labor contractual system, clarifying the rights and obligations of both parties of labor contracts, protecting the legitimate rights and interests of employees, and establishing and developing a harmonious and stable employment relationship.[283]

Therefore, this law aimed to improve the relationship between employers and employees by defining workers' rights and the duties of parties to labor contract.

---

[281] Wo Guo de Laodong Falu Zhidu 我国的劳动法律制度 (China's labor law system), Shi jie Quanguo Renda Changwei Hui Fazhi Jiangzuo Di Shiba Jiang 十届全国人大常委会法制讲座第十八讲 (The 18th lecture on the legal system of the Standing Committee of the 10th National People's Congress). Available at: http://www.npc.gov.cn/zgrdw/npc/xinwen/2006-03/21/content_347935.htm (Last Access: 29/04/2023)

[282] Garcia, Monique, *China's Labor Law Evolution: Towards A New Frontier*, ILSA Journal of Int'l & Comparative Law, Vol. 16:1, p. 237.

[283] Zhonghua Renmin GongheGuo Zhongyang Renmin Zhengfu 中华人民共和国中央人民政府 (The Central People's Government of the People's Republic of China), *Zhonghua Renmin Gingheguo Laodong Hetong Fa* 中华人民共和国劳动合同法 (*Labor Contract Law of the People's Republic of China*). Available at: http://www.gov.cn/flfg/2007-06/29/content_669394.htm

Translation in English: *Labor Contract Law of the People's Republic of China*, 29/06/2007. https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/76384/108021/F755819546/CHN76384%20Eng.pdf (Last Access: 24/05/2023)

To sum up, the Labor Law defines the rights and obligations of both parties and protect the legitimate rights and interests of workers, while the Labor Contract Law was adopted to ensure efficient implementation of the employment rules and principles mentioned in the labor law.[284]

Since this chapter mainly focuses on the impact of the PIPL on human resources management, not only the above-mentioned labor laws are important, but also the analysis of the Interim Regulation on Human Resources Market r*enli ziyuan shichang zanxing tiaoli* 人力资源市场暂行条例 is useful for the purpose of this paper.

The Interim Regulation on Human Resources Market which was signed by former Premier Li Keqiang 李克强 and came into force on October 1, 2018, is the first administrative regulation on job hunting, hiring and associated services in the human resources market.[285]

According to Article 1 of the Interim Regulation on Human Resources Market, this new regulation aims at regulating the market activities of human resources, promoting the rational flow and optimal allocation of human resources, facilitating employment and encouraging entrepreneurship.[286]

Article 29 of the Regulation is also very relevant, as it states that not only human resource service agencies that release human resource supply and demand information shall establish and improve information release review and complaint handling mechanisms to ensure that the released information is authentic, legal, and effective[287], but also that where human resource service agencies collect employer and personal information in business activities, they must not disclose or illegally use the business secrets and personal information they know.[288]

Therefore, the last part of the article – *bude xielou huozhe weifa shiyong suo zhixi de shangye mimi he geren xinxi* 不得泄露或者违法使用所知悉的商业秘密和个人信息 –

[284] Huang Donfil, *Labor Laws in China*, Doing Business in China, China Briefing. Available at: https://www.china-briefing.com/doing-business-guide/china/human-resources-and-payroll/labor-law (Last Access: 29/04/2023)
[285] China releases regulation on human resources market, China Daily, 17/07/2018. Available at: https://global.chinadaily.com.cn/a/201807/17/WS5b4d84b8a310796df4df6ea6.html (Last Access: 29/04/2023)
[286] Zhonghua Renmin Gongheguo Guowuyuan Ling 中华人民共和国国务院令，第 700 号 (Decree of the State Council of the PRC, n. 700), *Renli Ziyuan Shichang Zanxing Tiaoli* 人力资源市场暂行条例 *(Interim Regulation on Human Resources Market)*. Full text available at: http://www.gov.cn/zhengce/content/2018-07/17/content_5306967.htm
[287] Ibid.
[288] Ibid.

shows that there was already a first attempt to protect employer's and employee's personal information and to prevent disclosure (*xielu* 泄露) and illegal use (*weifa shiyong* 违法使用) of information.

The expression of personal information leakage – *geren xinxi xielu* 个人信息泄露 – was then used in the text of the PIPL (Article 51).

When dealing with employment relationship – that is the one between the employer and the employee – it is important to focus on the employer's responsibilities in handling employees' personal information.

Under the PIPL, employers are personal information handlers 个 *geren xinxi chulizhe* 人信息处理者, as they independently decide the purpose and method of processing and other personal information processing matters of the employees' personal information.[289]

As Article 3 of the PIPL states, where employers are registered outside the borders of the PRC, they are subject to PIPL compliance obligations in two circumstances:

1. Where the company provides products or services to individuals inside China;
2. Where the company analyzes and evaluates the activities of individuals inside China.

This aspect is similar to the *long-arm jurisdiction changbi guaxia* 长臂管辖 under the GDPR. In fact, before the GDPR went into effect, companies had to be compliant with the EU Data Protection Directive, which allowed organizations processing individuals' personal information to avoid compliance with the Directive by locating their business outside of the EU.

The GDPR's approach is different, as it takes into account not only the location of the processing but also the location of the individual whose personal data is being processed.[290]

Therefore, the territorial scope of the GDPR represents a significant evolution of the EU data protection law compared to the framework defined by Directive 95/46/EC.[291]

---

[289] Zhang, Fanny, Zhou Qian, *China's New Personal Information Protection Law: Impact on Employment Management*, China Briefing, 23/09/2021. Available at: https://www.china-briefing.com/news/chinas-new-personal-information-protection-law-impact-on-employment-management/ (Last Access: 03/05/2023)

[290] *The GDPR: Extending The Long Arm Of The Law*, Hong Kong Lawyer, 07/2018. Available at: https://www.hk-lawyer.org/content/gdpr-extending-long-arm-law (Last Access: 27/04/2023)

[291] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation, European Data Protection Board (edpb). Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf

Article 3 of the GDPR defines the territorial scope of the Regulation on the basis of two main criteria:

1. The establishment criterion. Article 3(1) states that the Regulation to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.[292]

2. The targeting criterion. Article 3(2) states that the Regulation applies to the processing of personal data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

b) the monitoring of their behavior as far as their behavior takes place within the Union.[293]

Moreover, Article 3(3) confirms the application of the GDPR to the processing where Member State law applies by virtue of public international law[294], as it states that the Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law[295].

Liu Chunquan 刘春泉, partner in the Intellectual Property Department of Duan & Duan Law Firm and deputy director of the Policy and Law Committee of the China Electronic Commerce Association, said in an interview with China Business News that "one aspect in which the major impact of the GDPR is that the GDPR adopts a legal model similar to the previous U.S. long-arm jurisdiction, which is not limited to EU enterprises, but extends the enforcement boundary to all enterprises in the EU."[296]

Article 13 of the PIPL provides that employers should not process the personal data of job applicants, current employees or former employees without having a lawful basis of

[292] General Data Protection Regulation GDPR. Available at: https://gdpr-info.eu/
[293] Ibid.
[294] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation, European Data Protection Board (edpb). Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf
[295] General Data Protection Regulation GDPR. Available at: https://gdpr-info.eu/
[296] *Shishang Zui Yan Shuju Baohu Fa An GDPR Zhengshi Shengxiao Chang Bi Guanxia Dianfu Ji You Shangye Moshi* 史上最严数据保护法案 GDPR 正式生效 "长臂管辖" 颠覆既有商业模式 (*The strictest data protection bill in history, GDPR, has come into force, and the "long arm jurisdiction" has disrupted the established business model*.), Xinliang Caijing 新浪财经 (Sina), 02/06/2018. Available at: http://finance.sina.com.cn/roll/2018-06-02/doc-ihcikcew5084521.shtml (Last Access: 03/05/2023)

processing.[297] The Article also states that the employer can only handle the information of prospective, current and former employees under the following circumstances:

1. Obtaining individuals' consent;
2. Where necessary to conclude or fulfill a contract in which the individual is an interested party, or where necessary to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded collective contracts;
3. Where necessary to fulfill statutory duties and responsibilities or statutory obligations;
4. Where necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions;
5. Handling personal information within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest;
6. When handling personal information disclosed by persons themselves or otherwise already lawfully disclosed, within a reasonable scope in accordance with the provisions of this Law.
7. Other circumstances provided in laws and administrative regulations[298].

In this Article it is possible to notice that, for the first time, being "necessary for human resources management" (*shishi renli ziyuan guanli suo bixu* 实施人力资源管理所必需) could be a lawful basis for processing personal information.[299] This aspect is beneficial to employers, as consent will be no longer needed for human resources management purposes.[300]

---

[297] Privacy Research Team, *Employee Personal Data Protection in China*, Securiti, 13/09/2021. Available at: https://securiti.ai/blog/employee-pipl/ (Last Access: 29/04/2023)

[298] Creemers, Rogier, Webster, Graham, Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)
Official text in Chinese: Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[298] Ibid.

[299] *Guide to China's Personal Information Protection Law (PIPL),* Dentons, 30/08/2021. Available at: https://www.dentons.com/en/insights/articles/2021/august/30/guide-to-chinas-personal-information-protection-law (Last Access 20/04/2023)

[300] Ibid.

The relationship between the employer and the employee is characterized by the collection of a big amount of personal information.

In fact, Article 8 of the Implementation Regulations for the PRC Labor Contract Law *zhonghua renmin gongheguo laodong hetongfa shishi tiaoli* 中华人民共和国劳动合同法实施条例 – formulated for the purpose of implementing the Labor Contract Law of the PRC – provides that a labor contract must contain the employee's personal information, including the name, ID card number, address, contact information, etc.[301]

Moreover, according to Article 72 of the Labor Law of the PRC, employers and employees must participate in social insurance and pay social insurance premiums.[302] As a consequence, companies are allowed to collect certain required personal information without consent when entering into labor contracts with their newly-recruited employees or when paying social insurance for their employees.[303]

However, the amount of information employers can handle is still limited by the principle of "purpose limitation and data minimization"; therefore, the processing of employees' personal information shall also be limited to a necessary scope.

An additional aspect which emerges from the analysis of Article 13 of the PIPL, is a difference with the GDPR: while in the EU regulation "legitimate interest" is considered a lawful basis for processing personal information, in the PIPL it is not.

Thus, under the PIPL, the employer (or any personal information handler) cannot claim that the processing is necessary for the purpose of the legitimate interests

pursued by the handler or a third party.[304]

---

[301] Zhonghua Renmin Gonheguo Guoyuan Ling 中华人民共和国国务院令, 第 535 号 (Decree of the State Council of the PRC, n. 535), *Zhonghua Renmin Gongheguo Laodong Hetongfa Shishi Tiaoli* 中华人民共和国劳动合同法实施条例 (*Implementation Regulations for the PRC Labor Contract Law*), 18/09/2008. Available at: http://www.gov.cn/zwgk/2008-09/19/content_1099470.htm

[302] Zhonghua Renmin Gongheguo Zhongyang Renmin Zhengfu 中华人民共和国中央人民政府 (The Central People-s Government of the PRC), *Zhonghua Renmin Gongheguo Laodongfa* 中华人民共和国劳动法 (*Labor Law of the PRC*), 05/07/1994. Available at: http://www.gov.cn/banshi/2005-05/25/content_905.htm

[303] *Personal information compliance in China in the context of employment*, Dentons, 1/03/2023. Available at: https://www.dentons.com/en/insights/articles/2023/march/1/personal-information-compliance-in-china-in-the-context-of-employment (Last Access: 04/05/2023)

[304] *Guide to China's Personal Information Protection Law (PIPL),* Dentons, 30/08/2021. Available at: https://www.dentons.com/en/insights/articles/2021/august/30/guide-to-chinas-personal-information-protection-law (Last Access 20/04/2023)

From the articles and regulations investigated above, it is possible to notice that the understanding of personal information and personal information processing is crucial to see how the management of employees' personal data works.

With a special focus on employment scenarios, every step of an employer's day-to-day labor management involves the collection and use of personal data.

There are different circumstances under which employers collect employees' data; for instance, when the employer requests an applicant to fill out a personal information form containing educational background, work experience, marital status and family background.[305]

Another example is when an employer monitors the employees' work computers and email system, as well as stored or transmitted data in the internal network.

Employees' data can also be collected in a non-competition investigation, through which the employer may engage investigators to track and take photographs of the employee to obtain evidence of their joining a competitor.

In human resources management activities, employees' personal information is characterized by a life cycle made of different phases, which goes from the collection to the deletion of data.

The first phase of this life cycle is collection: when a new employee is hired, important information is collected, including his or her name, the phone number, and the contact address.

The second phase is storage: when the employer inputs the employee's personal information onto the HR systems to increase the efficiency of administration.

The third phase is transfer: when the employer transfers the employee's personal information to a third party, e.g., an insurance company.

The fourth phase is deletion: when employers delete data that is no longer required or useful; for instance, where the employee leaves the company.

As it has been noted in paragraph 2.4 of this paper, when handling personal information, personal information processors must follow a series of principles.

As personal information handlers, employers must follow the above-mentioned principles in order to be compliant with the PIPL. In particular, two of these principles could be the

[305] Liu Tracy, Lian Larry, *PIPL impact on labour management and compliance*, Jingtian & Gongcheng, China Business Law Journal, 25/01/2023. Available at: https://law.asia/pipl-chinese-corporate-abour-management/ (Last Access: 05/05/2023)

most difficult to manage or the ones where disputes are easy to arise in human resources management: the principle of necessity and the principle of minimum.[306]

In their article for China Briefing, Fanny Zhang and Zhou Qian have provided an example of this.

Under some circumstances, for instance sick leave management, employees are usually asked to provide medical records in addition to the treatment registration slip and the sick leave recommendation note signed by the doctor. According to them, in this case, it is not clear if it can be considered as an excessive collection or if it violates the minimum principle.

Given the fact that there are no precedents at the moment, different interpretations can arise. Therefore, the two authors say that, because of this uncertainty, employers are suggested to take a cautious approach, review their current policy, and manage the information collection to reduce exposure to PIPL compliance risks.[307]

The PIPL's impacts on how a company's human resources department manages employees' data is huge and, in order to analyze it, different aspects must be taken into consideration: the cross-border transfer of employees' data, the lawful basis for personal information processing, and the management of employees' sensitive personal information.

3.2 Cross-border transfer of employees' personal information

The demand for cross-border transfer is growing, hence it has become a priority for lawmakers to consider when constructing related rules.[308]

The legal conditions for cross-border provision of personal information are the core content of the rules for cross-border provision of personal information, because they directly determine whether personal information can flow across borders[309].

---

[306] Zhang, Fanny, Zhou Qian, *China's New Personal Information Protection Law: Impact on Employment Management*, China Briefing, 23/09/2021. Available at: https://www.china-briefing.com/news/chinas-new-personal-information-protection-law-impact-on-employment-management/ (Last Access: 03/05/2023)

[307] Ibid.

[308] Zheng, Guan, *Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S. and China*, Computer Law & Security Review, Volume 43, 2021, 105610, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2021.105610, p. 1.

[309] He, Ran 赫然, *Geren Xinxi Kua Jing Tigong De Guifan Fenxi Yu Lilun Fansi – Yi "Geren Xinxi Baohu Fa" Di Sanshiba, Sanshijiu Tiao Wei Shijiao* 个人信息跨境提供的规范分析与理论反思 ——以《个人信息保护法》第三十八、三十九条为视角 (*Normative Analysis and Theoretical Reflection on the Cross-border Provision of Personal Information — From the Perspective of Articles 38 and 39 of the Personal Information Protection Law.*), Lanzhou Xue Kan 3 (2022): 97-105, p.4.

Moreover, such legal conditions reflect the effective balance between the free flow of personal information across borders and the legal values of rights protection, public security and national sovereignty.[310]

Multinational companies doing business in China are often involved in communication activities which go back and forth between the subsidiaries in China and the overseas headquarters.

As a consequence, when dealing with employees' personal data, employers not only have to put attention on how to collect and process sensitive personal information, but also on how to comply with the PIPL when transferring such information outside the borders of the PRC.

In addition, companies should know that if overseas employees remotely collect and process the personal information of Chinese users stored in China, it is also considered cross-border processing and is subject to the same requirements as if the company was transferring the personal information to overseas facilities.[311]

The rules on cross-border transfer of personal information are explained in Chapter III of the PIPL, in particular from Article 38 to Article 43.

Article 38 defines which are the conditions under which personal information handlers can transfer individuals' personal information outside the borders of the PRC.

Such conditions are:

1. Passing a security assessment organized by the State cybersecurity and informatization department according to Article 40 of this Law;
2. Undergoing personal information protection certification conducted by a specialized body according to provisions by the State cybersecurity and informatization department;
3. Concluding a contract with the foreign receiving side in accordance with a standard contract formulated by the State cyberspace and informatization department, agreeing upon the rights and responsibilities of both sides;

[310] Ibid.

[311] Huld, Arendse, *New Specifications for Cross-Border Processing of Personal Information for MNCs*, China Briefing, 11/05/2022. Available at: https://www.china-briefing.com/news/china-cross-border-personal-information-transfer-new-clarifications-for-multinational-companies/ (Last Access. 06/05/2023)

4. Other conditions provided in laws or administrative regulations or by the State cybersecurity and informatization department.[312]

To sum up these conditions, companies which want to legally transfer personal information abroad, can do so by choosing among three different procedures, according to the circumstances: passing the security assessment, signing a contract with the overseas receiving side or receiving a third-party certification. These three procedures will be analyzed in paragraph 3.2.1.

Article 39 states that personal information handlers who transfer individuals' personal information outside the borders of the PRC must notify PI subjects about the foreign recipient's name, contact method, handling purpose and methods, personal information categories, and the procedures for individuals to exercise their rights. Furthermore, they must obtain individuals' separate consent.

The informed-consent rule (*zhiqing tongyi guize* 知情同意规则) must also be observed in the cross-border provision of personal information, as the cross-border provision of personal information has a greater impact on the rights and interests of individuals.[313]

In fact, such processing will cause changes in the regulatory field, protection methods, and application of law, which will result in a weakening of control over personal information and protection of rights and interests of natural persons.[314]

In order to ensure that the rights and interests of natural persons' personal information are not reduced by cross-border flows, more stringent standards for the informed consent rule should be set. Such more stringent standards are reflected in two aspects.

---

[312] Creemers, Rogier, Webster, Graham, Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)
Official text in Chinese: Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[313] He, Ran 赫然, *Geren Xinxi Kua Jing Tigong De Guifan Fenxi Yu Lilun Fansi – Yi "Geren Xinxi Baohu Fa" Di Sanshiba, Sanshijiu Tiao Wei Shijiao* 个人信息跨境提供的规范分析与理论反思 ——以《个人信息保护法》第三十八、三十九条为视角 (*Normative Analysis and Theoretical Reflection on the Cross-border Provision of Personal Information — From the Perspective of Articles 38 and 39 of the Personal Information Protection Law.*), Lanzhou Xue Kan 3 (2022): 97-105, p.7.

[314] He, Ran 赫然, *Geren Xinxi Kua Jing Tigong De Guifan Fenxi Yu Lilun Fansi – Yi "Geren Xinxi Baohu Fa" Di Sanshiba, Sanshijiu Tiao Wei Shijiao* 个人信息跨境提供的规范分析与理论反思 ——以《个人信息保护法》第三十八、三十九条为视角 (*Normative Analysis and Theoretical Reflection on the Cross-border Provision of Personal Information — From the Perspective of Articles 38 and 39 of the Personal Information Protection Law.*), Lanzhou Xue Kan 3 (2022): 97-105, p.7.

First, the content of notification is expanded.[315] In fact, as it has already been said, Article 39 states that when a personal information processor provides personal information to foreign countries, it should notify the PI subject. This notification has a wider content, as it already includes the overseas recipients' information, processing purpose and methods, as well as procedures through which individuals can exercise their rights also with the foreign recipient. A wider notification content allows a greater protection of the rights of natural persons to exercise the rights of inquiry, reproduction, correction and supplement, deletion and other rights in the cross-border provision of personal information.[316]

Second, separate consent (*dandu tongyi* 单独同意) implies that personal information processors adopt a one-to-one approach with the PI subjects to obtain their consent.

Separate consent is likely to increase individuals' vigilance and attention, hence it can strengthen their awareness of personal information protection. Furthermore, separate consent can make PI subjects more cautious and rational when choosing to give their consent.

Although separate consent aims at protecting the right to self-determination of personal information, it will also increase the obligations and burdens of personal information processors, and may increase the difficulty and cost of cross-border provision of personal information.[317]

In addition, other drawbacks of separate consent can be identified.

First, it could it not be possible to effectively respond to the cross-border provision of personal information in emergency situations.[318]

For instance, if the cross-border provision and management of personal information of employees of multinational companies requires the individuals' consent (e.g., for health reasons), separate consent will not only increase the internal management and operating costs of the enterprise, but also bring more troubles to the employees themselves.

Another disadvantage is that other countries may adopt countermeasures in the flow of personal information. In this case, if other countries transfer their citizens' data to China,

---

[315] He, Ran 赫然, *Geren Xinxi Kua Jing Tigong De Guifan Fenxi Yu Lilun Fansi – Yi "Geren Xinxi Baohu Fa" Di Sanshiba, Sanshijiu Tiao Wei Shijiao* 个人信息跨境提供的规范分析与理论反思 ——以《个人信息保护法》第三十八、三十九条为视角 (*Normative Analysis and Theoretical Reflection on the Cross-border Provision of Personal Information — From the Perspective of Articles 38 and 39 of the Personal Information Protection Law.*), Lanzhou Xue Kan 3 (2022): 97-105, p.7.
[316] Ibid.
[317] Ibid.
[318] Ibid., p. 9.

they could adopt the principle of reciprocity and increase the conditions for exporting personal information, hence Chinese companies could have a competitive disadvantage in international trade.[319]

Article 41 of the PIPL states that, according to the principle of equality and mutual benefit, foreign judicial or law enforcements authorities' requests regarding the provision of personal information stored domestically will be held by competent authorities of the PRC.[320]

Therefore, when participating in judicial procedures or confronting administrative investigations outside of China, foreign companies should consider getting the relevant Chinese authority's approval on provision of personal information to overseas authorities.

Lastly, the restrictions stated by Article 41 also constitute a challenge for those companies conducting audits and investigations on their employees, in particular where legal enforcement agencies or judicial authorities are involved in such investigations and audits.[321]

According to Article 42 if foreign organizations or individuals handle personal information in such a way that harms national security or violates Chinese citizens' rights and interests, they can receive a warning or could be put on a list which limits or prohibits personal information provision by the State cybersecurity and informatization department.

Last article of the chapter – Article 43 – indicates which are the consequences in case of other countries' discriminatory behavior, e.g., discriminatory prohibitions or limitations. In this case, the PRC could adopt reciprocal measures against those countries.[322]

---

[319] He, Ran 赫然, *Geren Xinxi Kua Jing Tigong De Guifan Fenxi Yu Lilun Fansi – Yi "Geren Xinxi Baohu Fa" Di Sanshiba, Sanshijiu Tiao Wei Shijiao* 个人信息跨境提供的规范分析与理论反思 ——以《个人信息保护法》第三十八、三十九条为视角 (*Normative Analysis and Theoretical Reflection on the Cross-border Provision of Personal Information — From the Perspective of Articles 38 and 39 of the Personal Information Protection Law.*), Lanzhou Xue Kan 3 (2022): 97-105, p. 9.

[320] Creemers, Rogier, Webster, Graham, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)
Official text in Chinese: Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[321] *Impact of the new Personal Information Protection Law in the workplace*, Simmons+Simmons, 27/09/2021. Available at: https://www.simmons-simmons.com/en/publications/cku2ir2sx1gla0a019ycaji33/impact-of-the-new-personal-information-protection-law-in-the-workplace (Last Access: 06/05/2023)

[322] Creemers, Rogier, Webster, Graham, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)

Among all the Articles of Chapter III of the PIPL, Article 38 is the most relevant one, as it indicates the procedures through which employers can transfer employees' personal information outside the borders of the PRC. This aspect will be investigated in the following chapter.

3.2.1 The three conditions for cross-border data transfer (self-assessment, standard contract and PI certification)

When transferring employees' data – and in general individuals' personal information – outside the borders of the PRC, employers can choose among three different possibilities: passing the security assessment, signing a contract with the overseas receiving side or receiving a third-party certification.

Concerning the security assessment (*anquan pinggu* 安全评估), this condition sets up a prior administrative approval system for the implementation of cross-border provision of personal information by a specific subject, because the security assessment is only the means, it is not the final result of processing.

In fact, the competent unit needs to evaluate whether the cross-border personal information to be implemented by a specific subject meets the security standards, and on this basis make a decision on whether to allow the implementation of cross-border provision of personal information.[323]

On the one hand, the security assessment aims to maintain China's public security and national sovereignty, as well as to protect the rights and interests of natural persons' personal information. However, on the other hand, it may hinder the free flow of personal information across borders.

According to Article 40 of the PIPL, the scope of application of the security assessment is limited to two categories of personal information processors:

a) Critical information infrastructure operators;

[323] He, Ran 赫然, *Geren Xinxi Kua Jing Tigong De Guifan Fenxi Yu Lilun Fansi – Yi "Geren Xinxi Baohu Fa" Di Sanshiba, Sanshijiu Tiao Wei Shijiao* 个人信息跨境提供的规范分析与理论反思 ——以《个人信息保护法》第三十八、三十九条为视角 (*Normative Analysis and Theoretical Reflection on the Cross-border Provision of Personal Information — From the Perspective of Articles 38 and 39 of the Personal Information Protection Law.*), Lanzhou Xue Kan 3 (2022): 97-105, p. 4.

b) Personal information handlers who process a quantity of personal information which reaches the quantities provided by the State cybersecurity and informatization department.[324]

The term critical information infrastructure operators (CIIOs) *guanjian xinxi jichu sheshi* 关键信息基础设施 refer to information infrastructure in important sectors, e.g., energy, public communications, information services, transportation, finance. Given the relevance of such sectors, the destruction, loss or leakage of personal information could endanger national security, national economy and people's livelihood, and public interests.[325]

The Measures for the Security Assessment of Outbound Data *shuju chujing anquan pinggu banfa* 数据出境安全评估办法 – which aim to regulate outbound data transfer activities, protect personal information rights and interests, safeguard national security and the social public interest, and promote the secure and free cross-border flow of data[326] – provide some clarifications about the quantity of personal information above which the security assessment is required.

Article 4 of the Measures for the Security Assessment of Outbound Data states that the security assessment is required where:

1. Critical information infrastructure operators and data handlers handling the personal information of over 1 million people providing personal information abroad;
2. Data handlers provide abroad the personal information of more than 100,000 people or the sensitive personal information of more than 10,000 people since January 1 of the previous year.[327]

---

[324] Creemers, Rogier, Webster, Graham, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)

[325] He, Ran 赫然, *Geren Xinxi Kua Jing Tigong De Guifan Fenxi Yu Lilun Fansi – Yi "Geren Xinxi Baohu Fa" Di Sanshiba, Sanshijiu Tiao Wei Shijiao* 个人信息跨境提供的规范分析与理论反思 ——以《个人信息保护法》第三十八、三十九条为视角 (*Normative Analysis and Theoretical Reflection on the Cross-border Provision of Personal Information — From the Perspective of Articles 38 and 39 of the Personal Information Protection Law.*), Lanzhou Xue Kan 3 (2022): 97-105, p. 4.

[326] Zhonghua Renmin Gongheguo Guojia Hulianwang Xinxi Bangongshi 中华人民共和国国家互联网信息办公室 (Cybespace Administration of China), *Shuju Chujing Anquan Pinggu Banfa* 数据出境安全评估办法 (*Outbound Data Transfer Security Assessment Measures*), 07/07/2022. Available at: http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm

[327] Creemers, Rogier, Webster, Graham, Sacks, Samm, Laskai, Lorand, *Translation: Outbound Data Transfer Security Assessment Measures – Effective Sept. 1, 2022*, DigiChina, Stanford University, 08/07/2022. Available at: https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-effective-sept-1-2022/ (Last Access: 10/05/2023)

In addition, it is important to underline that although the term security assessment (安全评估) also appears in Article 36 of the PIPL, the two articles do not refer to the same type of security assessment.

Article 36 refers to an external assessment, which is conducted by the network information department on the export of personal information of network operators[328].

By contrast, Article 38 and 40 refer to a self-assessment conducted in advance by state agencies that provide personal information overseas[329].

According to Article 5 of the Measures for the Security Assessment of Outbound Data, when employers process and transfer employees' personal information outside China, they must conduct an outbound data transfer risk self-assessment.

Such outbound data transfer risk self-assessment shall be focused on six points, which are:

1. The legality, propriety, and necessity of the purpose and method of the outbound data transfer and data handling by the foreign receiving party;
2. The scale, scope, categories, and degree of sensitivity of the data transferred abroad; the risks that the outbound data transfer may engender to national security, the public interest, and the lawful rights and interests of individuals and organizations;
3. The responsibilities and duties undertaken and borne by the foreign receiving party, as well as whether or not the security of data transferred abroad can be ensured through management and technical measures and capabilities, etc., to fulfill their responsibilities and duties;
4. The risk of alteration, destruction, leak, loss, transfer, or illegal acquisition, illegal use, etc., during and after data is transferred abroad, and whether or not the channels to uphold personal information rights and interests are open, etc.;
5. Whether or not the data outbound transfer–related contract intended to be concluded with the foreign receiving party or another document with legal effect fully stipulates data security protection responsibilities and duties;

[328] He, Ran 赫然, *Geren Xinxi Kua Jing Tigong De Guifan Fenxi Yu Lilun Fansi – Yi "Geren Xinxi Baohu Fa" Di Sanshiba, Sanshijiu Tiao Wei Shijiao* 个人信息跨境提供的规范分析与理论反思 ——以《个人信息保护法》第三十八、三十九条为视角 (*Normative Analysis and Theoretical Reflection on the Cross-border Provision of Personal Information — From the Perspective of Articles 38 and 39 of the Personal Information Protection Law.*), Lanzhou Xue Kan 3 (2022): 97-105, p. 5.
[329] Ibid.

6. Other matters that may influence the security of data provision abroad.[330]

The second condition indicated by Article 38 of the PIPL refers to a personal information protection certification (*geren xinxi baohu renzheng* 个人信息保护认证); however, Article 38 of the law does not specify what this certification is nor how personal information handlers can obtain it.

This lack of information was solved on two occasions: first, November 18, 2022, when the CAC and the State Administration for Market Regulation (SAMR) emanated the Implementation Rules for Personal Information Protection Certification, also known as the PI Certification Rules[331]; and on December 16, 2022, when the National Information Security Standardization Technical Committee emanated the Network Security Standard Implementing Guidance – Certification Technical Specification for Cross-border Personal Information Transfers V2.0, also known as PI Certification Guidance V2.0.[332]

Furthermore, on March 16, 2023, the National Information Security Standardization Technical Committee also issued the Certification Requirements for Cross-Border Transmission of Personal Information[333] and solicited public comments, which can be submitted until May 15, 2023.

The above-mentioned documents provide further information on the PI Certification.

---

[330] Creemers, Rogier, Webster, Graham, Sacks, Samm, Laskai, Lorand, *Translation: Outbound Data Transfer Security Assessment Measures – Effective Sept. 1, 2022*, DigiChina, Stanford University, 08/07/2022. Available at: https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-effective-sept-1-2022/ (Last Access: 10/05/2023)

[331] Zhonghua Renmin Gongheguo Guojia Hulianwang Xinxi Bangongshi 中华人民共和国国家互联网信息办公室 (Cyberspace Administration of China), *Geren Xinxi Baohu Renzheng Shishi Guize* 个人信息保护认证实施规则 *(Implementation Rules for Personal Information Protection Certification),* 18/11/2022. Available at: http://www.cac.gov.cn/2022-11/18/c_1670399936983876.htm

[332] Quanguo Xinxi Anquan Biaozhunhua Jishu Weiyuanhui 全国信息安全标准化技术委员会 (National Information Security Standardization Technical Committee), *Wangluo Anquan Biaozhun Shijian Zhinan – Geren Xinxi Kua Jing Chuli Huodong Anquan Renzheng Guifan* 网络安全标准实践指南—个人信息跨境处理活动安全认证规范 (*the Network Security Standard Implementing Guidance – Certification Technical Specification for Cross-border Personal Information Transfers*), 16/12/2022. Available at: https://www.tc260.org.cn/upload/2022-12-16/1671179931039025340.pdf

[333] Quanguo Xinxi Anquan Biaozhunhua Jishu Weiyuanhui 全国信息安全标准化技术委员会 (National Information Security Standardization Technical Committee), *Guanyu Guojia Biaozhun《Xinxi Anquan Jishu Geren Xinxi Kua Jing Chuanshu Renzheng Yaoqiu》Zhengqiu Yijian Gao Zhengqiu Yijian De Tongzhi* 关于国家标准《信息安全技术 个人信息跨境传输认证要求》征求意见稿征求意见的通知 (*Notice on the national standard "Information Security Technology Personal Information Cross-border Transmission Authentication Requirements" draft for comments*), 16/03/2023. Available at: https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20230316143506&norm_id=20221102152946&recode_id=50381

Personal information protection certification refers to the opinion issued by a specialized certification body on whether the information processor's management system, operating conditions, product services, etc. meet the standards required by the personal information protection technical specification based on the relevant technical specifications.[334] Furthermore, this certification aims to ensure that companies comply with the PIPL and other relevant regulations while safeguarding the rights of personal information subjects during the transfer process.[335]

The domestic party of multinational companies which engage in personal information cross-border transfer between subsidiaries and parent company located in another country can apply for certification and bear legal responsibility on behalf of both parties.

Furthermore, overseas personal information handlers are allowed to request the certification through their specialized agencies or designated representatives established in China, which can assume legal responsibilities on their behalf.[336]

Lastly, only applicants who have legal personality, operate normally, and have a good reputation and goodwill can be eligible for the CAC certification.

After specifying who is eligible for the certification, the Certification Technical Specification for Cross-border Personal Information Transfers V2.0 defines which principles must be observed by personal information processors when engaging in cross-border personal information processing.

These principles include: the principles of lawfulness, propriety, necessity and good faith; the principles of openness and transparency; principle of information quality assurance; principle of equal protection; principle of clear responsibility and principle of voluntary certification.[337] Among these principles, the first three have already been analyzed in Chapter II of this paper, while the others are worth an analysis.

---

[334] He, Ran 赫然, *Geren Xinxi Kua Jing Tigong De Guifan Fenxi Yu Lilun Fansi – Yi "Geren Xinxi Baohu Fa" Di Sanshiba, Sanshijiu Tiao Wei Shijiao* 个人信息跨境提供的规范分析与理论反思 ——以《个人信息保护法》第三十八、三十九条为视角 (*Normative Analysis and Theoretical Reflection on the Cross-border Provision of Personal Information — From the Perspective of Articles 38 and 39 of the Personal Information Protection Law.*), Lanzhou Xue Kan 3 (2022): 97-105, p. 5.

[335] Zhang, Justina, *China's PI Certification for Cross-border Data Transfer: What You Need to Know*, GALA, 31/03/2023. Available at: http://blog.galalaw.com/post/102ibr9/chinas-pi-certification-for-cross-border-data-transfer-what-you-need-to-know (Last Access: 09/05/2023)

[336] Huld Arendse, *China's Draft Certification Standards for Cross-Border Personal Information Transfer*, China Briefing, 28/03/2023. Available at: https://www.china-briefing.com/news/draft-certification-standards-for-cross-border-processing-of-personal-information/ (Last Access: 10/05/2023)

[337] Quanguo Xinxi Anquan Biaozhunhua Jishu Weiyuanhui 全国信息安全标准化技术委员会 (National Information Security Standardization Technical Committee), *Wangluo Anquan Biaozhun Shijian Zhinan – Geren Xinxi Kua Jing Chuli Huodong Anquan Renzheng Guifan* 网络安全标准实践指南

The principle of equal protection (*tongdeng baohu yuanze* 同等保护原则) means that both the personal information processor and the overseas recipient must ensure the quality of the personal information in order to prevent adverse effects on the individuals' personal rights and interests. Moreover, it means that they must make sure that the cross-border processing of personal information meets the standards of the PIPL.

The principle of clear responsibility (*zeren mingque yuanze* 责任明确原则) means that both the personal information processor and the overseas recipient must designate a domestic party, multiple parties or an institution established by an overseas recipient in China to assume civil legal liability for the personal information processing activities of the overseas recipient in case of damage to individuals' rights and interests.

Last, the principle of voluntary certification (*ziyuan renzheng yuanze* 自愿认证原则) means to encourage personal information processors who engage in cross-border transfer of personal information to voluntarily apply for personal information protection certification. Furthermore, they must take advantage of the role of PI certification in increasing personal information protection and improving the efficiency of cross-border personal information processing.

In addition, the Security Certification Specifications also require personal information processors and their overseas recipients to sign legally binding and enforceable documents (*juyou falu yue shili de wenjian* 具有法律约束力的文件).

These documents constitute an agreement between the two parties (the processors and their overseas recipient) and are necessary to safeguard the protection of individuals' rights and interests during cross-border data transfer.

The binding document shall specify different elements, which are:

1. The basic information of the parties;
2. The details of the cross-border data transfer;
3. The responsibilities and obligations of the Parties to protect personal information;
4. The rights of PI subjects and how to protect them;
5. Clauses on remedy and dispute resolution;

—个人信息跨境处理活动安全认证规范 (*the Network Security Standard Implementing Guidance – Certification Technical Specification for Cross-border Personal Information Transfers*), 16/12/2022. Available at: https://www.tc260.org.cn/upload/2022-12-16/1671179931039025340.pdf

6. The overseas recipient's undertakings to comply with relevant PRC laws and regulations on PI protection and to accept continuous supervision by a certification agency;

7. Promises by the overseas recipient to accept the jurisdiction of Chinese laws and regulations on PI protection.

8. Statement of the organization which bears the legal responsibility within China, together with its promise to fulfil the obligations in order to protect personal information;

9. The Parties' entities in PRC who will bear legal liability for PI protection;

10. Other obligations as stipulated by applicable laws and regulations.[338]

Besides signing the above mentioned legally binding agreement, the personal information processor and its foreign recipient must designate a person with a deep knowledge of personal information protection – the Personal Information Protection Officer – who will take care of personal information protection and will have a decision-making position within the organization.

The Personal Information Protection Officer must undertake a series of responsibilities, such as clarifying which are the main goals, basic requirements and protection measures necessary for the PI protection; making sure that the human resources and financial resources within the company are adequate for the PI protection work; and reporting the PI protection work situation to the person in charge of the company.

The Security Certification Specifications also state that in order to prevent the leakage, loss or unauthorized access to personal information, the personal information processor and its overseas recipient shall establish a personal information agency (*geren xinxi baohu jigou* 个人信息保护机构) responsible for ensuring compliance with PI protection obligations.

This agency must formulate and implement a plan for cross-border personal information processing; organize a PI protection impact assessment; adopt all the necessary measures to ensure that the cross-border personal information is processed in accordance to the PI obligations; accept and handle personal information subjects' requests and complaints; and accept the certification bodies' supervision on personal information cross-border processing activities.

[338] Zhang, Justina, *China's PI Certification for Cross-border Data Transfer: What You Need to Know*, GALA, 31/03/2023. Available at: http://blog.galalaw.com/post/102ibr9/chinas-pi-certification-for-cross-border-data-transfer-what-you-need-to-know (Last Access: 09/05/2023)

Last, there must be a mutual agreement between the personal information processors and its overseas recipient upon the set of rules for cross-border personal information processing.

Now that the main obligations of both the personal information processor and its foreign recipient when engaging in cross-border PI processing have been clarified, an analysis of the PI certification process is necessary.

First of all, it is necessary to mention the CCRC – the China Cybersecurity Review Technology and Certification Centre *zhongguo wangluo Anquan shencha jishu yu renzheng zhongxin* 中国网络安全审查技术与认证中心 – which is the only official agency authorized to conduct the certification process for cross-border data transfer.[339]

After a consultation with the CCRC, the Global Advertising Lawyers Alliance (GALA) – an alliance of lawyers located all over the world – has found out that the PI certification process consists of different steps which have been summed up in Figure 1.

These steps include a preliminary review, an on-site inspection, and testing of relevant systems and processes.[340]

Furthermore, the CCRC requires no more than 110 working days to complete the process, but these days do not include the time required for the applicant's rectifications.

Lastly, Figure 1 also shows that after the certification is issued, the CCRC also conducts follow-up surveillance, as a way to ensure the continued compliance with the relevant regulations.[341]

[339] Zhang, Justina, *China's PI Certification for Cross-border Data Transfer: What You Need to Know*, GALA, 31/03/2023. Available at: http://blog.galalaw.com/post/102ibr9/chinas-pi-certification-for-cross-border-data-transfer-what-you-need-to-know (Last Access: 09/05/2023)
[340] Ibid.
[341] Ibid.

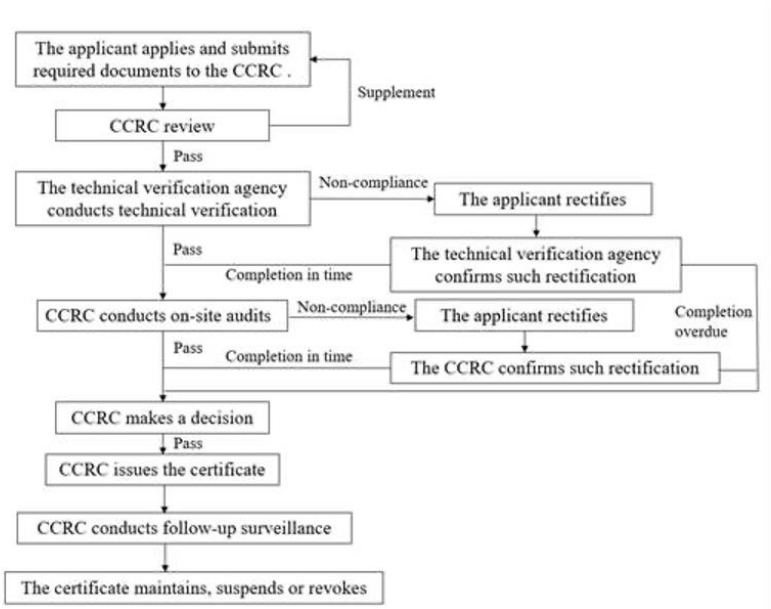

Figure 1. GALA, China's PI Certification for Cross-border Data Transfer: What You Need to Know[342]

In conclusion, when choosing among the three different strategies to legally transfer and process individuals' personal information outside the borders of the PRC, companies should keep in mind both the upsides and downsides of choosing to apply for PI Certifications.

On the one hand, PI Certifications are a useful framework for companies as they provide guidelines for all parties involved in cross-border data processing, e.g., certification agencies, personal information processors and overseas recipients, through which they can be aware of all their specific obligations.

Furthermore, PI Certifications can eliminate the information gap and technical inequality between information subjects and information processors by introducing professional and neutral third-party assessment and identification, and also contribute to healthy competition among information processors.[343]

[342] Zhang, Justina, *China's PI Certification for Cross-border Data Transfer: What You Need to Know*, GALA, 31/03/2023. Available at: http://blog.galalaw.com/post/102ibr9/chinas-pi-certification-for-cross-border-data-transfer-what-you-need-to-know (Last Access: 09/05/2023)

[343] He, Ran 赫然, *Geren Xinxi Kua Jing Tigong De Guifan Fenxi Yu Lilun Fansi – Yi "Geren Xinxi Baohu Fa" Di Sanshiba, Sanshijiu Tiao Wei Shijiao* 个人信息跨境提供的规范分析与理论反思 ——以《个人信息保护法》第三十八、三十九条为视角 (*Normative Analysis and Theoretical Reflection on the Cross-border Provision of Personal Information — From the Perspective of Articles 38 and 39 of the Personal Information Protection Law.*), Lanzhou Xue Kan 3 (2022): 97-105, p. 5.

However, on the other hand, since PI certification process in China is relatively new, companies could face different challenges and uncertainties associated with such process.[344]

Furthermore, the certification process can be time-consuming, expensing and risky, as business could not obtain certification because of a misunderstanding of the requirements.

Lastly, given that the PI certification process requires the cooperation between the personal information processor and its overseas recipient, another downside could be that obtaining the overseas recipients' cooperation could be challenging to obtain in some circumstances.

As a result, multinational companies should be aware of the above-mentioned factors when managing cross-border data transfer.

The third condition to legally transfer and process personal information outside the borders of the PRC is signing a contract with the foreign receiving side in accordance with a standard contract.

This procedure was clarified by the new Standard Contract Measures for the Export of Personal Information *geren xinxi chujing biaozhun hetong banfa* 个人信息出境标准合同办法[345], which were released by the CAC on February 22, 2023 and will come into effect on June 1, 2023.

The new Standard Contract Measures for the Export of Personal Information provide an explanation about which companies are eligible for this procedure and of the requisite contents of the contract itself.

Among the three alternative procedures provided by Article 38 of the PIPL, the Standard Contract is the simplest one, as it does not require an audit by either the CAC or a third-party agency.[346]

---

[344] Zhang, Justina, *China's PI Certification for Cross-border Data Transfer: What You Need to Know*, GALA, 31/03/2023. Available at: http://blog.galalaw.com/post/102ibr9/chinas-pi-certification-for-cross-border-data-transfer-what-you-need-to-know (Last Access: 09/05/2023)

[345] Zhonghua Renmin Gongheguo Guojia Hulianwang Xinxi Bangongshi 中华人民共和国国家互联网信息办公室 (Cybespace Administration of China), *Geren Xinxi Chujing Biaozhun Hetong Banfa* 个人信息出境标准合同办法 (*Standard Contract Measures for the Export of Personal Information*), 22/02/2023. Available at: http://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm

[346] Huld, Arendse, *Standard Contract Measures for Personal Information Export to Come into Force June 1*, China Briefing, 03/03/2023. Available at: https://www.china-briefing.com/news/china-data-transfer-personal-information-export-standard-contract-procedures/ (11/05/2023)

The Standard Contract *biaozhun hetong* 标准合同 differs from ordinary contracts in two aspects: first, from the subject of the standard contract is not one of the parties to the contract or a single party, but the State cyberspace and informatization department.[347]

Second, from the content point of view, given that the main subject of the standard contract is the State cyberspace and informatization department, which has a legal status detached from the parties concerned, therefore, the content of the Standard Contract is more objective and fairer. On the contrary, in an ordinary contract, the subject is usually a party with an economic advantage, which may take advantage of his dominant position to exempt itself from its obligations or increase the other party's responsibilities.[348]

Because of its simplified procedure, the Standard Contract condition can only be used by small data processors and processors who do not handle data related with national security and interests. In fact, Article 4 of the Standard Contract Measures for the Export of Personal Information provides a list of those who may provide personal information outside China by concluding standard contracts. This list includes:

1) Those who are not critical information infrastructure operators;
2) Those who handle the personal information of less than 1 million people;
3) Those who have cumulatively provided the personal information of fewer than 100,000 persons overseas since January 1, of the previous year;
4) Those who have cumulatively provided the sensitive personal information of fewer than 10,000 persons overseas since January 1, of the preceding year.[349]

Moreover, this Article also includes a clause which states that personal information processors are not allowed to split up the volume of personal information that ought to undergo a security review into smaller batches in order to be eligible for the Standard Contract procedure.[350]

---

[347] He, Ran 赫然, *Geren Xinxi Kua Jing Tigong De Guifan Fenxi Yu Lilun Fansi – Yi "Geren Xinxi Baohu Fa" Di Sanshiba, Sanshijiu Tiao Wei Shijiao* 个人信息跨境提供的规范分析与理论反思 ——以《个人信息保护法》第三十八、三十九条为视角 (*Normative Analysis and Theoretical Reflection on the Cross-border Provision of Personal Information — From the Perspective of Articles 38 and 39 of the Personal Information Protection Law.*), Lanzhou Xue Kan 3 (2022): 97-105, p. 5.
[348] Ibid.
[349] Measures on Standard Contracts for the Export of Personal Information, China Law Translate, 24/02/2023. Available at: https://www.chinalawtranslate.com/en/personal-information-export-contract/ (Last Access: 12/05/2023)
[350] Huld, Arendse, *Standard Contract Measures for Personal Information Export to Come into Force June 1*, China Briefing, 03/03/2023. Available at: https://www.china-briefing.com/news/china-data-transfer-personal-information-export-standard-contract-procedures/ (11/05/2023)

For what concerns the structure, the Standard Contract must adhere to the template provided along with the Standard Contract Measures. The Standard Contract consists of nine articles which include clauses about the two parties' obligations, the impact that the PI protection regulations in the area where the overseas recipient is located has on the fulfillment of the contract and the rights of the PI subjects.

Furthermore, according to Article 6 of the Standard Contract Measures, all the agreements between the Parties that are in conflict with the requirements of the Standard Contract template are not allowed.

The template provided by the CAC includes four required elements:

1. Basic information of the PI processor and the overseas recipient, e.g., the company names, addresses, contact persons' names, and contact information.
2. The length of the contract and mutual PI processing activity.
3. The technical and management measures employed by the overseas recipient in order to fulfill the obligations of the contract to protect PI and minimize security risks.
4. Agreed methods for arbitration and dispute resolution in event of a dispute.[351]

The Standard Contract Measures clarify how companies in China can handle cross border data transfer. Moreover, the contract template provided by the CAC is very helpful, as it explains what information each party must provide and which are the obligations that they are liable to.[352]

3.3 Conditions for Processing Employees' Sensitive Personal Information

The process of employees' sensitive personal information is another crucial aspect that should not be underestimated by employers.

Although according to Article 23 of the PIPL, in some cases employers do not need employees' consent when processing their information, the situation is different when the information to be processed is considered "sensitive" (*mingan* 敏感).

[351] Huld, Arendse, *Standard Contract Measures for Personal Information Export to Come into Force June 1*, China Briefing, 03/03/2023. Available at: https://www.china-briefing.com/news/china-data-transfer-personal-information-export-standard-contract-procedures/ (11/05/2023)
[352] Ibid.

Article 28 of the PIPL defines sensitive personal information *mingan geren xinxi* 敏感个人信息 as:

> personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14.[353]

Furthermore, Article 28 also states that an employer could handle employees' sensitive personal information only for a specific purpose and sufficient necessity, and only if strict protection measures have been taken.

To process employees' sensitive personal information, employers shall obtain employees' separate consent, and where laws or administrative regulations provide it, written consent shall also be obtained.

Moreover, when dealing with sensitive personal information, employers not only have to notify employees of information such as the name and contact method of the personal information handler, the purpose of personal information handling, handling methods and the retention period, but, according to Article 30, shall also notify individuals of the necessity and influence on the individual's rights and interests of handling the sensitive personal information.[354]

When analyzing the matter sensitive personal information, a comparison between the PIPL and the GDPR is necessary.

The main difference is that, while the PIPL defines such important data as "sensitive personal information", the GDPR – in particular Article 9 – refers to them as "special categories of personal data[355]".

---

[353] Creemers, Rogier, Webster, Graham, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)
Official text in Chinese: Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[354] Ibid.

[355] General Data Protection Regulation GDPR. Available at: https://gdpr-info.eu/

A similarity between the two regulations is that they both provide some specifications about the kind of information that must be considered as sensitive (in the PIPL) or special (in the GDPR).

Focusing on how the PIPL describes sensitive personal information, it is possible to notice how, among the other things, sensitive personal information refers to biometric data (*shengwu shibie xinxi* 生物识别信息), which includes those data used for facial and fingerprint recognition. As a consequence, employers should take special considerations when implementing surveillance measures.[356]

> The surveillance system in China is already well developed. Actually, in the construction of smart cities, mass surveillance serves to measure, track, and analyze data from various aspects of life including air quality and traffic congestion.[357]

The first element to analyze is facial recognition, which is undisputedly the most widely adopted artificial intelligence technology in China, having been applied in a wide range of sectors for a variety of purposes, ranging from facilitating identification to improving efficiency[358]. Moreover, facial recognition touches upon almost every aspect of an individual's life in China[359], and employment is no exception.

There are different cases that could be used as examples. To name one, tech company Canon has installed cameras with AI-enabled "smile recognition" technology in the offices of its Chinese subsidiary Canon Information Technology. These cameras only let smiling workers enter rooms or book meetings.

Given the huge impact that facial recognition has on Chinese citizens' life, the government has given huge importance to this new technology.

---

[356] Zhang, Thomas, *Personal Information Protection Law in China: Technical Considerations for Companies*, China Briefing, 8, 23, 2021. Available at: https://www.china-briefing.com/news/personal-information-protection-law-in-china-technical-considerations-for-companies/ (Last Access: 12/05/2023)

[357] Calzada, Igor, *Protecting smart city citizenship: Citizens' digital rights and AI-driven algorithmic disruption*, In Smart City Citizenship; Ed.; Elsevier Science Publishing Co Inc.: Cambridge, MA, USA, 2021, pp. 219–234. ISBN 9780128153000. https://doi.org/10.1016/B978-0-12-815300-0.00007-1

[358] Dudley, Lauren, *China's Ubiquitous Facial Recognition Tech Sparks Privacy Backlash*, THE DIPLOMAT, 07/03/2020, Available at: https://thediplomat.com/2020/03/chinas-ubiquitous-facial-recognition-tech-sparks-privacy-backlash/ (12/05/2023)

[359] Yan Luo, Rui Guo, *Facial Recognition in China: Current Status, Comparative Approach and the Road Ahead*, 25 U. Pa. J.L. & Soc. Change 153 (2022). Available at: https://scholarship.law.upenn.edu/jlasc/vol25/iss2/3

In fact, on July 2, 2021 the Supreme People's Court published a judicial interpretation[360] on the use of facial recognition technology for processing personal information.

According to this judicial interpretation, companies are required to disclose rules for the processing of facial information and expressly indicate the processing purpose, method and scope. Moreover, the use of bundling consent[361] for processing the users' facial information is not allowed.

As a consequence, when using facial recognition technologies in the workplace, employers should create standalone privacy notices for disclosing information related to facial recognition. Moreover, they must obtain employees' explicit separate consent for their facial information processing.

The second element to analyze are fingerprints. The use of this technology has a broader scope than the one of facial recognition.[362] In fact, in most cases, fingerprints are used to enter into buildings and offices.

When managing employees' fingerprints information, employers must adopt the same measures and considerations as the ones for facial recognition.

Another kind of personal information which is included in the biometric data is the one collected through CCTV cameras. In China, it is very common to distribute CCTV cameras around the business locations – e.g., the office or the factory – for security reasons.

If employers want to comply with the PIPL and avoid the violation of PI subjects' rights and interests, they shall be careful when monitoring the data collected by the CCTV cameras. In fact, monitoring data from CCTV cameras should be well managed and only a limited number of people should have access authorization to such data.[363]

---

[360] Zhonghua Renmin Gongheguo Zuigao Renmin Fayuan 中华人民共和国最高人民法院 (The Supreme People's Court of the PRC), Guanyu Shenli Shiyong Ren Lian Shibie Jishu Chuli Geren Xinxi Xiangguan Minshi Anjian Shiyong Falu Ruogan Wenti De Guiding 关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定 (Provisions on Several Issues Concerning the Application of Law in the Trial of Civil Cases Related to the Use of Face Recognition Technology to Handle Personal Information), 28/07/2021. Available at: https://www.court.gov.cn/fabu-xiangqing-315851.html

[361] Bundled consent refers to the practice of an organization 'bundling' together multiple requests for an individual's consent to a wide range of collections, uses and disclosures of personal information, without giving the individual the opportunity to choose which collections, uses and disclosures they agree to and which they do not.

[362] Zhang, Thomas, *Personal Information Protection Law in China: Technical Considerations for Companies*, China Briefing, 8, 23, 2021. Available at: https://www.china-briefing.com/news/personal-information-protection-law-in-china-technical-considerations-for-companies/ (Last Access: 12/05/2023)

[363] Ibid.

Thus, employers should adopt policies to regulate the usage, access and management of the data collected by the CCTV cameras, especially for those CCTV systems which upload personal information to external vendor over-the-air.[364]

In general, according to Article 26 of the PIPL, the installation of image collection or personal identity recognition equipment in public venues shall occur as required to safeguard public security and observe relevant State regulations, and clear indicating signs shall be installed. Moreover, collected personal images and personal distinguishing identity characteristic information can only be used for the purpose of safeguarding public security; it may not be used for other purposes, except where individuals' separate consent is obtained.[365]

Therefore, according to what this article states, separate consent is fundamental for employers to process employees' sensitive personal collected through the above-mentioned tools. It could be argued that it is a tradeoff between personal privacy and digital measurement.[366]

Employees' sensitive personal data may also be collected through electronic devices.

Based on the needs of enterprise management, when companies provide employees computers and mobile phones, it is also possible to set up monitoring software in them. Enterprises can use such software to understand the power on and off time of employees' computers and mobile phones, the browsing URL, and even the length of time the software is used. In some cases, companies monitor employees' mobile phone data usage through Wi-Fi monitoring and monitor the employees' position.

Some software companies have also developed remote clock-in functions. When employees visit customers, travel and work abroad, enterprises can require employees to

---

[364] Zhang, Thomas, *Personal Information Protection Law in China: Technical Considerations for Companies*, China Briefing, 8, 23, 2021. Available at: https://www.china-briefing.com/news/personal-information-protection-law-in-china-technical-considerations-for-companies/ (Last Access: 12/05/2023)

[365] Creemers, Rogier, Webster, Graham, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)
Official text in Chinese: Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[366] Kitchin, Rob, *Civil liberties or public health, or public liberties and public health? Using surveillance technologies to tackle the spread of COVID-19*, Space Polity 2020, 24, 362–381. https://doi.org/10.1080/13562576.2020.1770587

clock in at designated times and designated field locations to understand the actual situation of employees outside.[367]

Among the information and permissions that companies obtain through electronic devices, there are location information, hardware camera permissions, hardware storage permissions, hardware device information, etc.

With the advancement of technology, surveillance measures with higher efficiency and less cost will continue to be developed, and will be more widely applied in workplace.

When managing employees' personal information, lawfulness requirement is the first question that any processor shall take into careful consideration.

Furthermore, given that the PIPL does not admit "legitimate interest" as one lawful basis, employers in China are likely to rely more on employees' consent to meet the lawfulness requirement.[368]

The impact on the above-mentioned surveillance measures on the collection of employees' data and the importance of employees' consent for the collection of such data will be investigated in the following paragraphs.

3.4 Lawful bases for processing employees' personal information

With the rapid development and common use of digital technologies in China's workplace, employers' right to monitor and direct employees has often been abused, raising a number of disputes over infringement of employees' right to privacy[369].

As it was already mentioned in the previous paragraphs, nowadays a large amount of employees' information is collected and processed.

Employees are regularly subject to different types of investigation and electronic monitoring, e.g., telephone calls, detailed background checks, emails, and social media accounts.

---

[367] Qiye Ruhe Hegui Shouji Yuangong Geren Xinxi? 企业如何合规收集员工个人信息? (How companies collect employees' personal information in compliance?), Guo Feng Lushi Shiwu Suo 国枫律师事务所 (Grandway Law Offices), 09/05/2022. Available at: https://www.grandwaylaw.com/guofengshijiao/3716.html (Last Access: 15/05/2023)

[368] Sun, Yuchuan, *Legal Compliance of Workplace Surveillance in China -From a Personal Information Protection Perspective*, China Legal Newsletter, Hanling&Partners, July 2022. Available at: https://www.ohebashi.com/jp/newsletter/CN_NL_EN_Vol.2_Yuchuan%20Sun.pdf (Last Access: 15/05/2023)

[369] Zhang, Zhenxing, Zha, Yunfei, *The Systematic Construction of Lawfulness of Processing Employees' Personal Information Under the Chinese Personal Information Law*, 13/09/2022. Available at: http://dx.doi.org/10.2139/ssrn.4218180, p.1.

A widespread phenomenon in the workplace is the abuse of the right to human resources management, leading to issues such as information leakage, fraudulent use of employees' personal information or unlimited digital monitoring in the workplace.[370]

According to Zhenxing Zhang (Assistant Professor at Law school of Xi'an Jiaotong University) and Yunfei Zha (Assistant Professor at Guanghua Law school of Zhejiang University), it is crucial to find a balance between employers' right to monitor employees and employees' right to privacy. Furthermore, the two authors add, the balance between these two conflicting interests has become a universally controversial legal issue.[371]

With a special focus on China, Chinese Civil Code and the new Personal Information Protection Law can be considered as the primary legal source on which both employers and employee can rely when dealing with personal information protection.

When dealing with the lawfulness of processing employees' personal information, there is a big difference between the two regulations. Chinese Civil Code refers to a one-dimensional model, as it indicates consent as the only lawful basis for processing individuals' personal information.

In fact, Article 1035 indicates the conditions that shall be satisfied when processing personal information:

1. Consent has been obtained from the natural person or his guardian, unless otherwise provided by laws or administrative regulations;
2. The rules for processing information are publicized;
3. The purpose, method, and scope of the information processing are clearly indicated;
4. It is not in violation of laws or administrative regulations or against the agreement of both parties.[372]

By contrast, the PIPL – in particular Article 13 of the Law – identifies a three-dimensional model to determine the lawfulness of processing employees' personal information: this

[370] Zhang, Zhenxing, Zha, Yunfei, *The Systematic Construction of Lawfulness of Processing Employees' Personal Information Under the Chinese Personal Information Law*, 13/09/2022. Available at: http://dx.doi.org/10.2139/ssrn.4218180, p. 2.
[371] Ibid.
[372] Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People-s Congress of the PRC), Zhonghua Renmin Gongheguo Minfa 中华人民共和国民法典 Dian (Chinese Civil Code), 02/06/2020. Available at: http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml
English Translation: http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf

model includes employees' consent, the necessity for the conclusion or performance of an employment contract and necessity for conducting human resource management.[373]

Although the three-dimensional model has increased the importance given to the special needs of human resource management, Zhenxing Zhang and Yunfei Zha argue that it has to deal with the special issues deriving from the peculiarity of employment relations and lacks comprehensive understanding of the social-economic and informational asymmetry that characterize the relationship between the employer and the employee.

Furthermore, the two authors identified three main questions relating the effectiveness of the three-dimensional model and provided a number of cases related to electronic monitoring conducted by employers.

The first question is whether using employee consent as the primary source of lawfulness can be justified and how employee consent is related to the other two lawful bases.[374]

In reality, in China, before the PIPL came into effect, employers have always processed employees' personal information without obtaining their informed consent. Furthermore, judges have not checked whether employers had obtained employee consent when using video monitoring, nor whether the employee had sufficient freedom to make a meaningful choice in this matter.[375] Instead, the courts have simply confirmed the lawfulness of video and email surveillance videos on the basis of that the employer had a legitimate purpose for conducting these activities.

The example provided by the authors is the case Wu Zhongjun v Shenzhen Tengruifeng Technological Company[376]: the plaintiff argued that the employer's video monitoring on his work performance from May 22, 2018 to May 25, 2018 was conducted without his consent and violated his right to protection of personal information.

However, the Shenzhen Intermediate Court held that the evidences provided by the company (surveillance videos, emails and work diaries) proved that the employee had dealt with personal matters while at work and that his performance was poor.

---

[373] Zhang, Zhenxing, Zha, Yunfei, *The Systematic Construction of Lawfulness of Processing Employees' Personal Information Under the Chinese Personal Information Law*, 13/09/2022. Available at: http://dx.doi.org/10.2139/ssrn.4218180, p. 2-3.

[374] Ibid, p. 3.

[375] Ibid, p. 8.

[376] To read more about this case, please read: Wu Zhongjun, Shenzhenshi Tengruifeng Keji Youxian Gongsi Laodong Hetong Jiufen Ershen Minshi Panjueshu 吴仲军、深圳市腾瑞丰科技有限公司劳动合同纠纷二审民事判决书 (Wu Zhongjun, Shenzhen Tengruifeng Technology Co., Ltd. labor contract dispute second instance civil judgment), 30/06/2019. Available at: https://aiqicha.baidu.com/wenshu?wenshuId=f6849347470bda83ca78e96fc22a59009a7d502f

Therefore, although the court considered the evidences provided by the company as lawful, but failed to check whether the employer had employee consent for the video monitoring and if such consent was voluntary.

The second question that arises when dealing with the effectiveness of the three-dimensional model is when processing is based on the other two legal bases. In this case, it is unclear whether the employers have a duty of notification and, if it is not, how the employee's right to know might be safeguarded.[377]

Zhenxing Zhang and Yunfei Zha have noted how, in reality, employers have always processed employees' personal information without notification, and in many cases, the courts only analyzed whether employers had legitimate business interests to justify the processing of employee personal information, and did not check whether the employees had been informed of monitoring.

An example of this aspect is the case Xiu x v Rong x Plastic Knitting Packaging Company[378]: the employee argued that the company installed a hidden "Super-Eye Monitoring Software" on his computer without prior notification.

This software was then used by the employer to download the employee's messages on WeChat and QQ, and these acts violated the employee's right to personal information protection. However, although there was no prior notification of the installation of the above-mentioned software, the Yantai Intermediate Court in Shandong Province held that the installation, monitoring, the collection and storage of the employee's personal information were part of the enterprise management. As a consequence, they were considered as legitimate.

The third question that arises when analyzing the effectiveness of the three-dimensional model regards the standard of necessity. According to Zhenxing Zhang and Yunfei Zha, most Chinese courts only ask whether the employer had a legitimate business interest to justify the processing. They do not consider a series of questions which are relevant to the question

---

[377] Zhang, Zhenxing, Zha, Yunfei, *The Systematic Construction of Lawfulness of Processing Employees' Personal Information Under the Chinese Personal Information Law*, 13/09/2022. Available at: http://dx.doi.org/10.2139/ssrn.4218180, p. 9.

[378] To know more about this case, please read: Yuangong Xingwei Jiance Jiufen Anli: Qiye Liyong Ruanjian Jiankong Yuangong Diannao Shuyu Ziwo Guanli Hangwei, Bu Qinfan Yuangong Yinsiquan 员工行为监测纠纷案例：企业利用软件监控员工电脑属于自我管理行为，不侵犯员工隐私权 (Employee Behavior Monitoring Dispute Case: The use of software by an enterprise to monitor employees' computers is self-management and does not infringe upon employees' right to privacy), 23/02/2023. Available at: https://mp.weixin.qq.com/s?__biz=MzI5Nzc5MTI3MQ==&mid=2247513001&idx=1&sn=49d6fb054bd53717503e57ec5abcbee7&chksm=ecad49e1dbdac0f7309942b6f2d0511f96c21d4d2acee7cd4a05d01ba27bde848f705bff2b05&scene=27

of necessity, e.g., the extent of the monitoring, the availability of less intrusive methods, the degree of intrusion into employees' personal information interests and the seriousness of the consequences of monitoring.[379]

Also in this case, two cases can be analyzed to better understand the concept of necessity.

In the cases of Gao x v Wo x x (Yunnan) Commercial Retailing Co.Ltd Gejiu Jinhu Branch Store[380] and Wei Naicai v Hengtong Rubber Products (Shenzhen) Co., LTD[381], the courts – Honghe Intermediate People's Court and Shenzhen Intermediate People's Court, respectively – held that the surveillance videos provided by the companies proved that the employees had been absent from work or conducted strikes and slowdowns for many days. By doing so, the courts claimed, they caused the employers serious economic losses.

These two cases demonstrate that the courts confirmed the validity of the surveillance videos, but did not verify whether the video surveillance's purposes and means were legitimate and necessary or if the monitoring had violated the employees' privacy.

Moreover, what emerges from the cases analyzed above is that the majority of Chinese courts tend to give a broad and arbitrary interpretation and application of necessity. Chinese courts tend to have a form of employer favoritism which could be caused by the fact that Article 13, paragraph 2, subparagraph (2) of PIPL has no reference to the specific rules on assessing whether employers' processing has exceeded the extent of necessity.[382]

However, as Zhenxing Zhang and Yunfei Zha state, such employer favoritism should be criticized, not only because it puts the employees in a disadvantaged position, but also

---

[379] Zhang, Zhenxing, Zha, Yunfei, *The Systematic Construction of Lawfulness of Processing Employees' Personal Information Under the Chinese Personal Information Law*, 13/09/2022. Available at: http://dx.doi.org/10.2139/ssrn.4218180, p. 9.

[380] To read more about the case, please read: G Moumou, Woerma (Yunnan) Shangye Lingshou Youxian Gongsi Gejiu Jinhu Fendian Laodong Hetong Jiufen Ershen Minshi Panjueshu G 某某、沃尔玛（云南）商业零售有限公司个旧金湖分店劳动合同纠纷二审民事判决书 (G Moumou, Walmart (Yunnan) Commercial Retail Co., Ltd. San Francisco Branch Labor Contract Dispute Civil Judgment of Second Instance), 22/02/2019. Available at: https://aiqicha.baidu.com/wenshu?wenshuId=12760b9edf0cbab99554e50a0463f2e67f293e51

[381] To know more about the case, please read: Weinaicai Yu Hengtong Xiangjiao Zhipin (Shenzhen) Youxian Gongsi Laodong Zhengyi Ershen Minshi Panjueshu 韦乃财与恒通橡胶制品（深圳）有限公司劳动争议二审民事判决书 (Civil Judgment of Second Instance of Labor Dispute between Wei Naicai and Hengtong Rubber Products (Shenzhen) Co., Ltd.), 29/12/2014. Available at: https://aiqicha.baidu.com/wenshu?wenshuId=29660a4cff4ff18f63c4576f7e9511fc888d38d5

[382] Zhang, Zhenxing, Zha, Yunfei, *The Systematic Construction of Lawfulness of Processing Employees' Personal Information Under the Chinese Personal Information Law*, 13/09/2022. Available at: http://dx.doi.org/10.2139/ssrn.4218180, p. 16.

because it makes the relationship between the employer's interests and the employee's rights more unbalanced.[383]

After an analysis of the three questions on the effectiveness of the three-dimensional model, employees' consent is worth a deeper investigation, with a focus on whether consent as a primary lawful basis is sufficient for employees' personal information processing.

Article 14 of the PIPL states that:

> consent shall be given by individuals under the precondition of full knowledge, and in a voluntary and explicit statement.[384]

Therefore, a valid employee consent must be characterized by two elements: first, it can be given only with sufficient information to make informed decisions about the processing of personal information[385]; second, valid consent can only be given with complete autonomy and freedom.[386]

For what concerns the precondition of full knowledge, Zhenxing Zhang and Yunfei Zha argue that employees' right to know can be questioned on two aspects. The first one is that employees' right to know lacks procedural guarantees against employers' arbitrariness.[387]

Given the differential bargaining power of employers and employees, the formulation, the content and the disclosure of employees' personal information rules cannot be left in the hands of employers.

Furthermore, in general, employers do not formulate personal information processing rules, and, if they do, such rules are usually meaningless and just symbolic, as they are not put forward to employees, nor are the results of a negotiation with the labor units.

The second aspect worth mentioning when analyzing employees' right to know, it that employees' right to be informed is difficult to achieve due to the opacity and complexity of

---

[383] Zhang, Zhenxing, Zha, Yunfei, *The Systematic Construction of Lawfulness of Processing Employees' Personal Information Under the Chinese Personal Information Law*, 13/09/2022. Available at: http://dx.doi.org/10.2139/ssrn.4218180, p. 16.

[384] Creemers, Rogier, Webster, Graham, Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)
Official text in Chinese: Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[385] Zhang, Zhenxing, Zha, Yunfei, *The Systematic Construction of Lawfulness of Processing Employees' Personal Information Under the Chinese Personal Information Law*, 13/09/2022. Available at: http://dx.doi.org/10.2139/ssrn.4218180, p. 11.

[386] Ibid.

[387] Ibid, p. 12.

digital technologies and the informational asymmetries between employers and employees.[388]

In fact, employers tend to take advantage of digital technologies – such as algorithm or office automatic system – to collect and handle employees' personal information without prior notification and without employees' informed consent.

For what concerns employees' freedom and autonomy to give consent, in China, given the power imbalance between employers and employees, employees' consent is often given under coercive power without true autonomy and freedom.[389] In fact, employees often choose to give consent processing activities for fear of losing the job or losing investment in promotion, welfare, etc.

Not only employees accept to give their consent for fear, but they can be convinced by employers who use their coercive power to influence their choice.

Employers' coercive power can be used in a positive and negative way: the former refers to incentives (such as giving applicants an entry-level job or increasing the employees' annual bonus) aimed to persuade the employees to give their consent to personal information processing. The latter consists of using threats (such as firing the employee or reducing his annual bonus) to persuade employees to five their consent to personal information processing.

In conclusion, it is possible to notice how in most cases employees' consent is not given in full freedom and autonomy, hence consent as a primary lawful basis is not sufficient for personal information processing.

In fact, as Pauline T. Kim – Professor at Washington University School of Law – states, in the employment context, freedom of employee consent may be illusory.[390]

This analysis on the PIPL's three-dimensional model for personal information processing, and, in particular, on employees' consent, the following paragraph will focus on how employees' consent affects the employer's possibility to use the employees' collected data as evidence during a labor dispute.

---

[388] Zhang, Zhenxing, Zha, Yunfei, *The Systematic Construction of Lawfulness of Processing Employees' Personal Information Under the Chinese Personal Information Law*, 13/09/2022. Available at: http://dx.doi.org/10.2139/ssrn.4218180, p. 12.

[389] Ibid, p. 13.

[390] Kim, Pauline T., *Privacy Rights, Public Policy, and the Employment Relationship*, Ohio State Law Journal 57.3 (1996), p. 720.

3.4.1 The use of employees' WeChat data as evidence in disputes without consent: a Beijing Fengtai District People's Court case

In most companies, it is common for employers to provide employees with company devices – e.g., laptops, mobile phones, tablets – for work-related purposes.[391]

In addition, employers use different methods to monitor the activities on the company devices provided to employees in order to protect proprietary information.

The data obtained from a company device can be used as evidence in two circumstances: in case of an internal investigation or when there is a dispute.

In case of a labor dispute, one question arises: where is the boundary of the employer's right to collect and process the personal information of the workers based on the right of employment management?[392]

A recently reported case could be used to answer to this question: an employee (the Plaintiff) has signed two consecutive fixed-term labor contracts with an environmental protection company (the Defendant). Before the second labor contract expired, the company decided not to renew the open-ended labor contract on the grounds that the employee violated the company's policy.

However, the employee believed that there was no violation of the company's policy and that the company's decision not to renew the contract should be considered as an illegal termination of the labor contract which sought financial damages. As a consequence, he decided to appeal to the court.

The company claimed that the employee engaged in a number of non-compliant activities[393], including the falsification of sick leave and fraudulent leave, which breached the company's reward and punishment system regulations. Moreover, another allegation is that the employee handled personal matters during working hours and lied to the company

[391] Huang, Bill, Ligorner, K Lesli, *Beijing Courts Find Wechat Records Inadmissible If Recovered Without Employee Consent,* Morgan Lewis, 19/04/2023. Available at: https://www.morganlewis.com/pubs/2023/04/beijing-courts-find-wechat-records-inadmissible-if-recovered-without-employee-consent#_ftn1 (Last Access: 28/04/2023)

[392] Yongren danwei Shanzi Huifu de Yuangong Weixin Liaotian Jilu Nengfou Zuowei Shuju 用人单位擅自恢复的员工微信聊天记录能否作为证据？ (Can the employees' Wechat chat records restored by the employers without authorization be used as evidence?), Mingli Zhian 明理之案, 24/03/2023. Available at: https://baijiahao.baidu.com/s?id=1761248862658232832 (Last Access: 26/04/2023)

[393] Huang, Bill, Ligorner, K Lesli, *Beijing Courts Find Wechat Records Inadmissible If Recovered Without Employee Consent,* Morgan Lewis, 19/04/2023. Available at: https://www.morganlewis.com/pubs/2023/04/beijing-courts-find-wechat-records-inadmissible-if-recovered-without-employee-consent#_ftn1 (Last Access: 28/04/2023)

about this by colluding with another employee.[394] To prove it, the company submitted the WeChat records regarding the conversation of the employee and his colleague which were collected from the company computer used by the employee.

When questioned how they obtained the WeChat records, the company first answered that they recovered (without consent) the deleted data on the company computer used by the employee. Later, the company claimed that the WeChat records were collected by another employee with the employee's consent, but they did not provide any documentation to support this contrary account.[395]

The trial court – Beijing Fengtai District People's Court *beijing fengtaiqu renmin fayuan* 北京市丰台区人民法院 – found in favor of the employee and supported all his claims. Moreover, the court refused to admit the WeChat records between the employee and the co-worker, as the company failed to prove that they were legally collected.

In a separate paragraph in the judgement about the collection of deleted data by the company, the trial court pointed that regardless of the contents of the deleted WeChat records from the company computer, they constitute the employee's personal information and should have been collected only after the employee provided his informed consent in a voluntary and explicit manner.[396]

Furthermore, the trial court not only criticized the use of the employees' personal data as evidence in the dispute, but it also requested that the company increases its awareness of personal information protection and fulfills its responsibilities to protect the employees' rights.

The company filed an appeal to the Beijing Secondary Intermediate People's Court *beijingshi di erzhongji renmin fayuan* 北京市第二中级人民法院 which affirmed the trial court's decision in February 2022.

The Beijing Secondary Intermediate Court (also known as the Beijing Intermediate Court) has given great importance to judicial research work and has formed a number of highly

[394] Huang, Bill, Ligorner, K Lesli, *Beijing Courts Find Wechat Records Inadmissible If Recovered Without Employee Consent,* Morgan Lewis, 19/04/2023. Available at: https://www.morganlewis.com/pubs/2023/04/beijing-courts-find-wechat-records-inadmissible-if-recovered-without-employee-consent#_ftn1 (Last Access: 28/04/2023)
[395] Ibid.
[396] Ibid.

professional research results around the frontier issues of theory and practice and in-depth analysis of cases[397], and this Beijing Fengtai District People's Court case is no exception.

After its affirmation of the trial court's decision, the Beijing Intermediate Court conducted a study based on the above case.

This study – which was awarded the second prize of the 2022 Excellent Case Analysis of the National Court System *quanguo fayuan xitong* 全国法院系统[398] – the Beijing Intermediate Court analyzes the boundaries for employers to lawfully collect and process employees' personal information.[399]

The study conducted by the Beijing Intermediate Court provides some key guidelines for labor dispute cases.

The first one is that in labor dispute cases, the court should not ignore the rights and interests of employees' personal information protection due to the right of employment management, and should review the employer's information handling behavior through three aspects: legality (*hefaxing* 合法性), legitimacy (*zhengdangxing* 正当性) and reasonableness (*helixing* 合理性), and determine the admissibility of the evidence obtained through such activities accordingly.[400]

When dealing with legality, informed consent is a fundamental factor and – as it has already been noted in the previous paragraph – it is the primary condition for employers to process employees' personal information.

Article 13 of the PIPL states that the labor contract can be considered as a general authorization to the employer, as the contract can be regarded as a form of general consent

---

[397] Yongren danwei Shanzi Huifu de Yuangong Weixin Liaotian Jilu Nengfou Zuowei Shuju 用人单位擅自恢复的员工微信聊天记录能否作为证据？ (Can the employees' Wechat chat records restored by the employers without authorization be used as evidence?), Mingli Zhian 明理之案, 24/03/2023. Available at: https://baijiahao.baidu.com/s?id=1761248862658232832 (Last Access: 26/04/2023)

[398] To know all the winners, please read: Quanguo Fayuan Xitong 2022 Niandu Youxiu Anli Fenxi Pingxuan Huojiang Mingdan 全国法院系统 2022 年度优秀案例分析评选获奖名单 (National Court System 2022 Excellent Case Analysis Award Winner List). Available at: https://www.163.com/dy/article/HPU7DGMV051486CM.html (Last Access: 03/05/2023)

[399] Huang, Bill, Ligorner, K Lesli, *Beijing Courts Find Wechat Records Inadmissible If Recovered Without Employee Consent,* Morgan Lewis, 19/04/2023. Available at: https://www.morganlewis.com/pubs/2023/04/beijing-courts-find-wechat-records-inadmissible-if-recovered-without-employee-consent#_ftn1 (Last Access: 28/04/2023)

[400] Yongren danwei Shanzi Huifu de Yuangong Weixin Liaotian Jilu Nengfou Zuowei Shuju 用人单位擅自恢复的员工微信聊天记录能否作为证据？ (Can the employees' Wechat chat records restored by the employers without authorization be used as evidence?), Mingli Zhian 明理之案, 24/03/2023. Available at: https://baijiahao.baidu.com/s?id=1761248862658232832 (Last Access: 26/04/2023)

provided by the employee for processing personal information that is necessary for the purpose of employment management.[401]

However, the processing of any personal information beyond this specific purpose and of employees' sensitive personal information requires informed consent.

The second important element to analyze is legitimacy. Legitimacy is related to the purpose of the processing. When dealing with the purposes of processing, three aspects should be taken into consideration:

1. The collection of personal information and the purpose of subsequent processing must be compatible.[402]

When their personal information is collected by employers, employees must be clearly informed about the purpose, reason and scope of the collection of their data. Furthermore, there must be a correlation between the scope of the information collection and the scope of its subsequent processing. In the study conducted by the Beijing Intermediary Court, an example is provided to explain this aspect: if an employer collects medical examination information for the purpose of ensuring labor safety, but subsequently uses the medical examination information as a tool to evaluate the performance of the workers and support the termination of the worst performer, not only the purpose of collecting and using the information differs greatly and exceeds the expected use of medical examination information by the employees, but it also violates the principle according to which the purpose should be clear and specific.

2. The purposes for employees' personal information processing must be acceptable.[403]

The purpose of collecting information by the employer is required to be acceptable, which means that full consideration must be given to the needs of employment management.

To explain this concept, another example is provided: an employer's installation of GPS positioning systems on the company car and video surveillance in the office space are legitimate if the application's purpose is to ensure that the company equipment is properly

---

[401] Huang, Bill, Ligorner, K Lesli, *Beijing Courts Find Wechat Records Inadmissible If Recovered Without Employee Consent,* Morgan Lewis, 19/04/2023. Available at: https://www.morganlewis.com/pubs/2023/04/beijing-courts-find-wechat-records-inadmissible-if-recovered-without-employee-consent#_ftn1 (Last Access: 28/04/2023)

[402] Yongren danwei Shanzi Huifu de Yuangong Weixin Liaotian Jilu Nengfou Zuowei Shuju 用人单位擅自恢复的员工微信聊天记录能否作为证据？ (Can the employees' Wechat chat records restored by the employers without authorization be used as evidence?), Mingli Zhian 明理之案, 24/03/2023. Available at: https://baijiahao.baidu.com/s?id=1761248862658232832 (Last Access: 26/04/2023)

[403] Ibid.

used and safely kept. However, if this installation's purpose is to pry into employees' privacy or to collect evidence for potential litigation in the future, it will exceed the normal work needs and seriously infringe on the boundaries of employees' personal information. As a consequence, the Beijing Intermediate Court clearly states that where in a potential litigation the evidence materials are collected by the employer in this way, these evidences should not be accepted by the court.

3. The processing of employees' personal information must be relevant to employment management.[404]

Being relevant to the employment management means that the processing of employees' personal information must be based on labor needs and that employers shall not carry out information activities beyond its business scope. To examine whether the employers' information processing behavior is relevant to employment management, the court should make a comprehensive judgement based on different factors, e.g., the employer's business scope, specific scenarios, labor positions, and policy requirements.

To better explain this concept, another example is provided: there are some circumstances under which employers need to collect employees' health information to know whether they have infectious diseases or other diseases that are not compatible with the job position, for instance in the case of chefs or waiters engaged in catering work. However, for those employees engaged in non-front-line positions, the collection of this type of information is not necessary, hence is not legitimate.

When dealing with employers' personal information handling behavior, the third and last element to take into consideration is reasonableness. Reasonableness should be evaluated based on whether the processing is proportionate.[405]

The principle of proportionality requires that employers should collect personal information only to the minimum extent necessary for achieving employment management purposes.[406]

---

[404] Yongren danwei Shanzi Huifu de Yuangong Weixin Liaotian Jilu Nengfou Zuowei Shuju 用人单位擅自恢复的员工微信聊天记录能否作为证据？ (Can the employees' Wechat chat records restored by the employers without authorization be used as evidence?), Mingli Zhian 明理之案, 24/03/2023. Available at: https://baijiahao.baidu.com/s?id=1761248862658232832 (Last Access: 26/04/2023)

[405] Huang, Bill, Ligorner, K Lesli, *Beijing Courts Find Wechat Records Inadmissible If Recovered Without Employee Consent,* Morgan Lewis, 19/04/2023. Available at: https://www.morganlewis.com/pubs/2023/04/beijing-courts-find-wechat-records-inadmissible-if-recovered-without-employee-consent#_ftn1 (Last Access: 28/04/2023)

[406] Huang, Bill, Ligorner, K Lesli, *Beijing Courts Find Wechat Records Inadmissible If Recovered Without Employee Consent,* Morgan Lewis, 19/04/2023. Available at:

The principle of proportionality (*biliyuanze* 比例原则) does not explicitly appear in the PIPL; hence it is not among those principles which were analyzed in paragraph 2.4 of this paper. However, according to the Beijing Intermediate Court, the expressions contained in Article 6 of the PIPL "*adopt methods that have the least impact on individuals' rights and interests*"[407] and "*the collection of personal information shall be limited to the minimum scope of achieving the purpose of processing, and personal information shall not be excessively collected*"[408] are essentially embodied in the principle of proportionality.[409]

When dealing with the concept of reasonableness, the relationship between damage (*sunhai* 损害) and gain (*shouyi* 收益) should be considered. In fact, the gain of the employer's right of employment management right is achieved through the employee's damage of part of his or her personal information rights and interests.[410]

In practice, employers control the flexibility and scale of management methods; while employees' dependence on employers reduces employees' vigilance against personal information protection. Furthermore, information asymmetry between employer and employee and the technical barriers increase the difficulty for employees to discover employers' infringements.

Therefore, the Beijing Intermediate Court states that the court can judge the reasonableness of the information processing behavior by whether the degree of damage to the rights and interests of the employee is proportional to the benefit obtained by the employer.[411]

---

https://www.morganlewis.com/pubs/2023/04/beijing-courts-find-wechat-records-inadmissible-if-recovered-without-employee-consent#_ftn1 (Last Access: 28/04/2023)

[407] Creemers, Rogier, Webster, Graham, Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)
Official text in Chinese: Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[408] Ibid.

[409] Yongren danwei Shanzi Huifu de Yuangong Weixin Liaotian Jilu Nengfou Zuowei Shuju 用人单位擅自恢复的员工微信聊天记录能否作为证据？ (Can the employees' Wechat chat records restored by the employers without authorization be used as evidence?), Mingli Zhian 明理之案, 24/03/2023. Available at: https://baijiahao.baidu.com/s?id=1761248862658232832 (Last Access: 26/04/2023)

[410] Ibid.

[411] Yongren danwei Shanzi Huifu de Yuangong Weixin Liaotian Jilu Nengfou Zuowei Shuju 用人单位擅自恢复的员工微信聊天记录能否作为证据？ (Can the employees' Wechat chat records restored by the employers without authorization be used as evidence?), Mingli Zhian 明理之案, 24/03/2023. Available at: https://baijiahao.baidu.com/s?id=1761248862658232832 (Last Access: 26/04/2023)

In conclusion, after the above considerations, an overview of the investigated case can be provided.

It is clear that the employer is in a dominant position in the labor relationship and that the employer and the employee belong to an unequal relationship of continuous information. This inequality becomes crucial in cases of disputes and litigation between the two parties, as the employer can access to a wide amount of the employees' personal information, even without the employee's informed consent.

However, the above-mentioned case and the subsequent analysis conducted by the Beijing Intermediate Court demonstrate that only if the employee's information is collected in accordance to the principles of legitimacy, legality and reasonableness, it can be used as evidence in a labor dispute between the two parties.

Conclusions

The main purpose of this thesis was to provide an overview of the Personal Information Law, as since its promulgation it has led to different changes in the way companies – both domestic and foreign – manage their business operations.

Through the analysis conducted in the three chapters that constitute this thesis, different considerations can be made.

First of all, China – as well as the majority of countries of the world – has attached great importance to the development of a data protection regulation. This growing concern over data is caused by different elements. To name one, a strong data protection regulation stimulates consumer trust and the use of digital tools which promote investment, competition and innovation in the digital economy. Another reason is that a strong data protection regulation can reduce risks such as the loss, misuse or theft of data. Moreover, nowadays data protection regulations are considered as strategic tools to protect national security.

However, it could also be argued that such regulations could be considered as trade barriers and the different approach towards data management adopted by governments may also lead to political tensions. An example of this matter can be provided by the growing trade tensions between China and US which led to the imposition of sanctions by both governments. Data governance and protection is one of the reasons behind such tensions. The most recent – and maybe known – case is that of the Chinese company TikTok (in China *Douyin* 抖音) which is considered by many countries as a risk to national security. Thus, many countries such as Australia, Canada, US, all members of the EU, have imposed limitations on TikTok. The reason of such bans is that Western countries fear that the parent company of TikTok Bytedance, could share users' data with Chinese government if requested to do so.

In fact, the main difference between Western countries' regulations on data protection, e.g., the GDPR, and China's PIPL as well as the other regulations, is that in countries such as US or EU members, everyone is subject to the law, including the government which cannot force a company to share the collected data. However, this is not the case in China. In fact, although different articles of the PIPL – e.g., Article 33 – state that the Law applies to State organs' handling activities, Western governments argue that the Chinese Party could force Chinese companies to release the data they collected and such companies are not allowed to refuse.

In fact, Article 63 of the PIPL states that when State authorities fulfill their duties and responsibilities (for instance, through on-site inspections) to investigate whether a party has unlawfully handled personal information, the concerned parties cannot obstruct or impede the State authorities to do so; on the contrary, they must cooperate with them.

Another important consideration which emerges from this analysis is the unequal and unbalanced relationship between the personal information handler and the personal information subject. Although the new regulations aim to protect individuals' rights, underline personal information handlers' duties and strengthen the legal liabilities in case of an unlawful handling of personal data, such unbalanced relationship still exists. As it was seen in Chapter III, such inequality is what characterizes the relationship between employer and employee. Moreover, it also characterizes the between companies and users, whose data is used to improve the companies' marketing strategies. Companies still collect and process a huge amount of personal information and they way such information is handled has an impact on individuals. Although the amount of personal information has been limited by the regulations and companies are forced to be compliant with the laws, the personal information subjects still find themselves in a disadvantageous position.

In conclusion, this thesis provides further evidence of how crucial the role of data is today. It is not a matter which affects one sector only, but the number of areas influenced by the management of big data constantly grows. This is why the regulations such as the PIPL or the GDPR are just the starting point of the ongoing effort made by regulators to keep up with technological development. The Artificial Intelligence Act of the EU and the Measures for the Management of Generative Artificial Intelligence Services (*sheng chengshi rengongzhineng fuwu guanli banfa* 生成式人工智能服务管理办) are two examples of such process.

References

Administrative Punishments Law of the PRC (2021 edition), China Law Translate, 22/01/2021. Available at: https://www.chinalawtranslate.com/en/administrative-punishment-law-2021/#_Toc62220180 (Last Access 23/03/2023)

Aimei Zixun (iiMedia)艾媒咨询，*2021 Nian Zhongguo Shuzihua Yingxiao Hangye Yanjiu Baogao* 2021 年中国数字化营销行业研究报告 (*China Digital Marketing Industry Research 2021 Report*), 18/01/2022. Available at: https://www.iimedia.cn/c400/83281.html (Last Access: 14/04/2023)

Aimin Qi, Guosong Shao, Wentong Zheng, *Assessing China's Cybersecurity Law*, Computer Law & Security Review, Volume 34, Issue 6, 2018, p. 1342-1354, ISSN 0267-3649. https://doi.org/10.1016/j.clsr.2018.08.007

Bartosik-Purgat, Małgorzata, Ratajczak-Mrożek, Milena, *Big Data Analysis as a Source of Companies' Competitive Advantage: A Review*., Entrepreneurial Business and Economics Review 6.4 (2018): 197-215.

Beijing Huagong Daxue 北京化工大学 (Beijing University of Chemical Technology), Guanyu Xinxi Anquan Dengji Baohugongzuo De Shishi Yijian 关于信息安全等级保护工作的实施意见 (Implementation Opinions concerning the Information Security Multi-Level Protection System), 14/09/2012. Available at: https://cit.buct.edu.cn/2012/0914/c7951a95007/page.htm

Bennett, Susan, *Risk Management: Data as a Strategic National Resource - the Importance of Governance and Data Protection*., Governance Directions 71.7 (2019): 362-66.

Calzada, Igor, *Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)*, Smart Cities 2022, 5, 1129–1150. https://doi.org/10.3390/smartcities5030057

Calzada, Igor, *Data Co-operatives through Data Sovereignty*, Smart Cities 2021, 4, 1158–1172. https://doi.org/10.3390/smartcities4030062

Calzada, Igor, *Protecting smart city citizenship: Citizens' digital rights and AI-driven algorithmic disruption*, In Smart City Citizenship; Ed.; Elsevier Science Publishing Co Inc.: Cambridge, MA, USA, 2021, pp. 219–234. ISBN 9780128153000.

Chen, Jiayao, *Economic Thinking of Big Data Killing in the Internet Era*, 2021, In: Abawajy, J., Choo, KK., Xu, Z., Atiquzzaman, M. (eds) 2020 International Conference on Applications and Techniques in Cyber Intelligence. ATCI 2020. Advances in Intelligent Systems and Computing, vol 1244. Springer, Cham. https://doi.org/10.1007/978-3-030-53980-1_142

Cheng Jihong, Liu Lianshi, Wei Longjie 陈际红, 刘连炻, 韦龙杰, *Quanzhi Qingzhong, Duzhi Zhangduan: Ruhe Kaizhan Geren Xinxi Baohufa Xiang Xia de Hegui Shenji*? 权知轻重，度知长短：如何开展《个人信息保护法》项下的合规审计? (*Right to know the weight, right to know the length: How to conduct a compliance audit under the Personal Information Protection Law?*), Zhong Lun 中伦, 10/05/2022. Available at: https://www.zhonglun.com/Content/2022/05-10/1542310423.html (Last Access: 21/03/2023)

China Briefing Team, *China's Personal Information Protection Law: A Comparison of the First Draft, the Second Draft, and the Final Document*, China Briefing, 24/08/2021. Available at: https://www.china-briefing.com/news/chinas-personal-information-protection-law-a-comparison-of-the-first-draft-the-second-draft-and-the-final-document/ (Last Access 16/05/2023)

China releases regulation on human resources market, China Daily, 17/07/2018. Available at: https://global.chinadaily.com.cn/a/201807/17/WS5b4d84b8a310796df4df6ea6.html Last Access: 29/04/2023)

Cong Gerenxinxi Baohufa Ancao Ershengao Bianhua Kan Lifaqushi Ji Hegui Yaodian 从个人信息保护法草案二审稿变化看立法趋势及合规要点 (*Legislative trends and compliance points from the changes in the second draft of the Personal Information Protection Law*), Simmons&Simmons, 08/05/2021. Available at: https://www.simmons-simmons.com/en/publications/cktbiji8f1zsm0a42cpz5heqb/simmons-data-observation-4 (Last Access 18/05/2023).

Creemers, Rogier, *China's Emerging Data Protection Framework*, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac011, p. 1. Available at: https://doi.org/10.1093/cybsec/tyac011

Creemers, Rogier, *Implementation Opinions concerning the Information Security Multi-Level Protection System*, China Copyright and Media, The Law and policy media in China, 14/09/2012. Available at: https://chinacopyrightandmedia.wordpress.com/2004/09/15/implementation-opinions-concerning-the-information-security-multi-level-protection-system/ (Last access 18/05/2023)

Creemers, Rogier, *Personal Information Protection Law (Expert Suggestion Draft)*, DigiChina, Stanford University, 17/10/2019. Available at: https://digichina.stanford.edu/work/personal-information-protection-law-expert-suggestion-draft/ (Last access 18/05/2023)

Creemers, Rogier, Webster, Graham, Sacks, Samm, Laskai, Lorand, *Translation: Outbound Data Transfer Security Assessment Measures – Effective Sept. 1, 2022*, DigiChina, Stanford University, 08/07/2022. Available at: https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-effective-sept-1-2022/ (Last Access: 10/05/2023)

Creemers, Rogier, Webster, Graham, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DigiChina, Stanford University, 20/08/2022. Available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Last Access: 28/05/2023)

Data bureau to help build digital society, The State Council of The People's Republic of China (English.gov.cn), 09/03/2023. Available at: https://english.www.gov.cn/news/topnews/202303/09/content_WS64091edec6d0a757729e7e16.html (Last Access: 22/03/2023)

DiDi. *Milestones*, https://www.didiglobal.com/about-special/milestone (Last Access: 04/04/2023)

Donnelly, Drew, China Social Credit System Explained – What is it & How Does it Work?, Horizons, 06/04/2023. Available at: https://nhglobalpartners.com/china-social-credit-system-explained/ (Last Access: 26/03/2023)

Dudley, Lauren, *China's Ubiquitous Facial Recognition Tech Sparks Privacy Backlash*, THE DIPLOMAT, 07/03/2020, Available at: https://thediplomat.com/2020/03/chinas-ubiquitous-facial-recognition-tech-sparks-privacy-backlash/ (12/05/2023)

European Union, *Digital Market Act*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925

European Union, *Digital Services Act*. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022R2065

Foreign Investment Law of the People's Republic of China, National Development and Reform Commission (NDRC) People's Republic of China, 24/02/2021. Available at: https://en.ndrc.gov.cn/policies/202105/t20210527_1281403.html

G Moumou, Woerma (Yunnan) Shangye Lingshou Youxian Gongsi Gejiu Jinhu Fendian Laodong Hetong Jiufen Ershen Minshi Panjueshu G 某某、沃尔玛（云南）商业零售有限公司个旧金湖分店劳动合同纠纷二审民事判决书 (G Moumou, Walmart (Yunnan) Commercial Retail Co., Ltd. San Francisco Branch Labor Contract Dispute Civil Judgment of Second Instance), 22/02/2019. Available at: https://aiqicha.baidu.com/wenshu?wenshuId=12760b9edf0cbab99554e50a0463f2e67f293e51

Garcia, Monique, *China's Labor Law Evolution: Towards A New Frontier*, ILSA Journal of Int'l & Comparative Law, Vol. 16:1.

General Data Protection Regulation GDPR Fines/Penalties, Intersoft Consulting. Available at: https://gdpr-info.eu/issues/fines-penalties/#:~:text=83(4)%20GDPR%20sets%20forth,fiscal%20year%2C%20whichever%20is%20higher (Last Access 22/03/2023)

General Data Protection Regulation GDPR. Available at: https://gdpr-info.eu/

Geren Xinxi Baohufa Dui Qiye de Shi Da Yingxiang《个人信息保护法》对企业的十大影响 (*Ten Big Effects of the Personal Information Protection Law on Enterprises*), Zhongguo Zhongxiao Qiye Guoji Hezuo Xiehui 中国中小企业国际合作协会 (International Cooperation Association of SMEs), 27/8/2021. Available at: https://xiehui.chinasme.org.cn/site/content/8594.html (Last Access: 24/03/2023)

Geren Xinxi Baohufa Shishi Hou HulianWang Guanggao de Weilai Zai Nali? 个人信息保护法实施后，互联网广告的未来在哪里？ (*How is the future of Internet advertising after the implementation of the Personal Information Protection Law?)* https://new.qq.com/rain/a/20211102A0A7O000 (Last Access: 21/04/2023)

Ghosh, Soumik, *How China's Information Protection Law Affects Businesses,* Bankinfosecurity, 09/09,2021. Available at: https://www.bankinfosecurity.asia/how-chinas-information-protection-law-affects-businesses-a-17498 (Last Access: 17/03/2023)

Goswami, Swish, "The Rising Concern Around Consumer Data and Privacy", *Forbes*, 14/12/2020. Available at: https://www.forbes.com/sites/forbestechcouncil/2020/12/14/the-rising-concern-around-consumer-data-and-privacy/ (Last Access 17/05/2023)

Greenleaf, Graham, *China's Completed Personal Information Protection Law: Rights Plus Cyber-security*, 172 Privacy Laws & Business International Report 20-23, UNSW Law Research Paper No. 21-91, 2021, p. 6. http://dx.doi.org/10.2139/ssrn.3989775

Guanyu Tuijin Geren Xinxi Baohu Hegui Shenji de Ruogan Jianyi 关于推进个人信息保护合规审计的若干建议 (*Some Suggestions on Promoting Compliance Audits of Personal Information Protection*), Geren Xinxi Baohu Hegui Shenji Tuijin Xiaozu 个人信息保护合规审计推进小组 (Personal Information Protection Compliance Audit Promotion Team), December 2021. Available at: https://sjc.nju.edu.cn/_upload/article/files/3f/8e/7c88cdb5453c81bb8ba3c3c7671a/113a2ae6-0d26-4c97-8d5d-6715e94740b8.pdf (Last Access: 21/03/2023)

Guanyu Xinxi Anquan Dengji Baohugongzuo De Shishi Yijian 关于信息安全等级保护工作的实施意见 (Implementation Opinions concerning the Information Security Multi-Level Protection System), 15/09/2004. Available at: https://chinacopyrightandmedia.wordpress.com/2004/09/15/implementation-opinions-concerning-the-information-security-multi-level-protection-system/

Guide to China's Personal Information Protection Law (PIPL), Dentons, 30/08/2021. Available at: https://www.dentons.com/en/insights/articles/2021/august/30/guide-to-chinas-personal-information-protection-law (Last Access 20/04/2023)

Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation, European Data Protection Board (edpb). Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf

Guojia Hulianwang Xinxi Bangongshi Youguan Fuzeren Jiu Dui Didi Quanqiu Gufen Youxian Gongsi Yifa Zuochu Wangluo Anquan Shencha Xiangguan Xingzheng Chufa de Jueding Da Jizhe Wen 国家互联网信息办公室有关负责人就对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定答记者问 (*The relevant person in charge of the Cyberspace Administration of China answered reporters' questions on the decision to impose administrative penalties related to the cybersecurity review of Didi Global Co., Ltd*. in accordance with the law), 21/07/2022. Available at: http://www.cac.gov.cn/2022-07/21/c_1660021534364976.htm (Last Access: 05/04/2023)

He, Ran 赫然, *Geren Xinxi Kua Jing Tigong De Guifan Fenxi Yu Lilun Fansi – Yi "Geren Xinxi Baohu Fa" Di Sanshiba, Sanshijiu Tiao Wei Shijiao* 个人信息跨境提供的规范分析与理论反思 ——以《个人信息保护法》第三十八、三十九条为视角 (*Normative Analysis and Theoretical Reflection on the Cross-border Provision of Personal Information — From the Perspective of Articles 38 and 39 of the Personal Information Protection Law.*), Lanzhou Xue Kan 3 (2022): 97-105.

Hong Yanqing 洪延青, Wangluo Anquan Fa Dui Shuju Anquan Baohu Zhi De Yu Shi 《网络安全法》对数据安全保护之得与失 (On the Gain and Loss of Cybersecurity Law of China on Data Protection). Zhengce Pinglun 政策评论 (Pol Rev) 2017;1: 66–73. http://library.ttcdw.com/uploadfiles/zk/1507792951.pdf

How to Leverage Private Domain Traffic in China, The Egg. Available at: https://www.theegg.com/social/china/how-to-leverage-private-domain-traffic/#:~:text=What%20is%20private%20domain%20traffic,to%20communicate%20with%20this%20audience (Last Access 16/04/2023)

Huang Donfil, *Labor Laws in China*, Doing Business in China, China Briefing. Available at: https://www.china-briefing.com/doing-business-guide/china/human-resources-and-payroll/labor-law (Last Access: 29/04/2023)

Huang, Bill, Ligorner, K Lesli, *Beijing Courts Find Wechat Records Inadmissible If Recovered Without Employee Consent*, Morgan Lewis, 19/04/2023. Available at: https://www.morganlewis.com/pubs/2023/04/beijing-courts-find-wechat-records-inadmissible-if-recovered-without-employee-consent#_ftn1 (Last Access: 28/04/2023)

Huang, Yehan, Shi, Mingli, *Top Scholar Zhou Hanhua Illuminates 15+ Years of History Behind China's Personal Information Protection Law*, DigiChina, Stanford University, 8/06/2012. Available at:

https://digichina.stanford.edu/work/top-scholar-zhou-hanhua-illuminates-15-years-of-history-behind-chinas-personal-information-protection-law/ (Last Access 15/05/2023)

Huld Arendse, *China's Draft Certification Standards for Cross-Border Personal Information Transfer*, China Briefing, 28/03/2023. Available at: https://www.china-briefing.com/news/draft-certification-standards-for-cross-border-processing-of-personal-information/ (Last Access: 10/05/2023)

Huld, Arendse, *How Did Didi Run Afoul of China's Cybersecurity Regulators? Understanding the US$1.2 Billion Fine*, China Briefing, 2/08/2022. Available at: https://www.china-briefing.com/news/didi-cyber-security-review-which-laws-did-didi-break/ (Last Access: 04/04/2023)

Huld, Arendse, *New Specifications for Cross-Border Processing of Personal Information for MNCs*, China Briefing, 11/05/2022. Available at: https://www.china-briefing.com/news/china-cross-border-personal-information-transfer-new-clarifications-for-multinational-companies/ (Last Access. 06/05/2023)

Huld, Arendse, *Standard Contract Measures for Personal Information Export to Come into Force June 1*, China Briefing, 03/03/2023. Available at: https://www.china-briefing.com/news/china-data-transfer-personal-information-export-standard-contract-procedures/ (11/05/2023)

Impact of the new Personal Information Protection Law in the workplace, Simmons+Simmons, 27/09/2021. Available at: https://www.simmons-simmons.com/en/publications/cku2ir2sx1gla0a019ycaji33/impact-of-the-new-personal-information-protection-law-in-the-workplace (Last Access: 06/05/2023)

Jay, Pil Choi, Doh-Shin, Jeon, Byung-Cheol, Kim, *Privacy and personal data collection with information externalities,* Journal of Public Economics, Volume 173, 2019, pp. 113-124, https://doi.org/10.1016/j.jpubeco.2019.02.001

Jia, Jingxin 贾婧欣, *Qiye Weifa Chuli Geren Xinxi Xingzheng Chufa de Guanxiaquan Zhengyi* 企业违法处理个人信息行政处罚的管辖权争议 (*Jurisdictional disputes over administrative penalties for the handling of personal information by enterprises in violation of the law*), Jingji Yanjiu Daokan 经济研究导刊 (Journal of Economic Research) 19 (2022): 153-55. Available at: https://kns.cnki.net/kcms2/article/abstract?v=P6B9XB_UHltA7AHkgT6aKGT5VUiIdBwI2eq6UI19NMIZYgCU13MGE4yl6x8w1WqAGKJj9KQBSZ_LwcOzkO-TCBeVzaIPosJhMeLdS_8c1wcL_kSFh261eQU2MtdqtpsI&uniplatform=NZKPT

Jiang, Bixin 江必新, *Xingzheng Chufa Fa Tiaowen Jingshi Yu Shili Jingjie* 行政处罚法条文精释与实例精解, (*Detailed interpretation of the provisions and examples of the Administrative Punishment Law*) Beijing 北京：Renmin Fayuan Chubanshe 人民法院出版社 (People's Court Press), 2021: 7.

Jin, Yuxin, Skiera, Bernd, *How Do Privacy Laws Impact the Value for Advertisers, Publishers and Users in the Online Advertising Market? A Comparison of the EU, US and China*, Journal of Creating Value, 8(2), 306–327, 2022. https://doi.org/10.1177/23949643221117676

Jingzhun Yingxiao Moshi Shoucuo Xin Jishu Qianghua Yinsi Baohu Hou ge Baohu Shidai Shuzi Guanggao Hangye Zhe Ji Haishi Biange 精准营销模式受挫，新技术强化隐私保护，后个保法时代数字广告行业折戟还是变革？ (*The precision marketing model has suffered setbacks, and new technologies have strengthened privacy protection. Will the digital advertising industry collapse or change in the post-law protection era*?), Shiji Jingji Baodao 21 世纪经济报道 21 (21st Century Business Herald), 7/11/2022. Available at: https://m.21jingji.com/article/20221107/herald/aa25db972571ed7c9a557332e02463ec_zaker.html (Last Access: 20/04/2023)

Jingzhun Yingxiao Moshi Shoucuo Xin Jishu Qianghua Yinsi Baohu Hou ge Baohu Shidai Shuzi Guanggao Hangye Zhe Ji Haishi Biange 精准营销模式受挫，新技术强化隐私保护，后个保法时代数字广告行业折戟还是变革？ (*The precision marketing model has suffered setbacks, and new technologies have strengthened privacy protection. Will the digital advertising industry collapse or change in the post-law protection era?*), 21 Shiji Jingji Baodao 21 世纪经济报道 (21st Century Business Herald), 7/11/2022. Available at: https://m.21jingji.com/article/20221107/herald/aa25db972571ed7c9a557332e02463ec_zaker.html (Last Access: 21/04/2023)

Junhe 君和, *"Gebaofa" Mantan Xilie Zhiyi: Liaoliao Shuju Kexidaiquan Jiang Ruhe Luodi*《个保法》漫谈系列之一：聊聊数据可携带权将如何落地 (*One of a series of talks on the Personal Insurance Law: Talking about how the right to data portability will be implemented*), 22/08/2021. Available at: http://www.junhe.com/legal-updates/1538 (Last Access 28/05/2023).

Kim, Pauline T., *Privacy Rights, Public Policy, and the Employment Relationship*, Ohio State Law Journal 57.3 (1996), p. 720.

Kipfer, Arlo, *China's New Personal Information Protection Law Forced Out Yahoo and Linkedin: Will YOU Be Next*, China Law Blow, Harris Bricken, 11/09/2021. Available at: https://harrisbricken.com/chinalawblog/chinas-new-personal-information-protection-law-forced-out-yahoo-and-linkedin-will-you-be-next/ (Last Access: 11/04/2023)

Kitchin, Rob, Civil liberties or public health, or public liberties and public health? Using surveillance technologies to tackle the spread of COVID-19, Space Polity 2020, 24, 362–381. https://doi.org/10.1080/13562576.2020.1770587

Kumar, V., Bharath Rajan, *What's in It for Me? The Creation and Destruction of Value for Firms from Stakeholders*, Journal of Creating Value 3.2 (2017): 142-56.

Labor Contract Law of the People's Republic of China (English Translation), 29/06/2007. https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/76384/108021/F755819546/CHN76384%20Eng.pdf (Last Access: 24/05/2023)

Lee, Alexa, Shi, Mingli, Chen, Qiheng, Horsley, Jamie P., Schaefer, Kendra, Creemers, Rogier, Webster, Graham, Seven Major Changes in China's Finalized Personal Information Protection Law, DigiChina, Stanford University, 15/09/2021. Available at: https://digichina.stanford.edu/work/seven-major-changes-in-chinas-finalized-personal-information-protection-law/ (Last Access 16/05/2023)

Li, Yiqiang, *Challenges Under New Personal Information Protection Regime in China*, Faegre Drinker, 25/8/2021. Available at: https://www.faegredrinker.com/en/insights/publications/2021/8/challenges-under-new-personal-information-protection-regime-in-china (Last Access: 26/03/2023)

Li, Yiqiang, *Challenges Under New Personal Information Protection Regime in China*, Faegre Drinker, 25/8/2021. Available at: https://www.faegredrinker.com/en/insights/publications/2021/8/challenges-under-new-personal-information-protection-regime-in-china (Last Access: 06/05/2023)

Li, Yixi, Wang, Meiyu, *Restore Customer Trust and Public Reputation: Case Study of Didi*, Proceedings of the 2022 7th International Conference on Financial Innovation and Economic Development (ICFIED 2022), 26/3/2022. Available at: https://www.atlantis-press.com/proceedings/icfied-22/125971978 Last Access: 04/04/2023)

Liang, Fan, Vishnupriya Das, Nadiya Kostyuk, and Muzammil M. Hussain, *Constructing a Data -Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, Policy and Internet 10.4 (2018): 415-53.

Liu Tracy, Lian Larry, *PIPL impact on labour management and compliance*, Jingtian & Gongcheng, China Business Law Journal, 25/01/2023. Available at: https://law.asia/pipl-chinese-corporate-abour-management/ (Last Access: 05/05/2023)

Liu, Jinhe, *China's data localization*, Chinese Journal of Communication, 13, 1-20, 2019. https://doi.org/10.1080/17544750.2019.1649289

Measures on Standard Contracts for the Export of Personal Information, China Law Translate, 24/02/2023. Available at: https://www.chinalawtranslate.com/en/personal-information-export-contract/ (Last Access: 12/05/2023)

Personal information compliance in China in the context of employment, Dentons, 1/03/2023. Available at: https://www.dentons.com/en/insights/articles/2023/march/1/personal-information-compliance-in-china-in-the-context-of-employment (Last Access: 04/05/2023)

Polina, Rebeka, *China's Personal Information Protection Law (PIPL): Is Your Business Ready for It?*, The Sumsuber, 25/01/2022. Available at: https://sumsub.com/blog/china-personal-information-protection-law/#twelfth (Last Access: 22/03/2023)

Privacy Research Team, *Employee Personal Data Protection in China*, Securiti, 13/09/2021. Available at: https://securiti.ai/blog/employee-pipl/ (Last Access: 29/04/2023)

Privacy Research Team, *The HR Guide to Employee Data Protection*, Securiti, 26/08/2022. Available at: https://securiti.ai/blog/hr-employee-data-protection/ (Last Access: 28/05/2023)

Qiye Ruhe Hegui Shouji Yuangong Geren Xinxi? 企业如何合规收集员工个人信息? (How companies collect employees' personal information in compliance?), Guo Feng Lushi Shiwu Suo 国枫律师事务所 (Grandway Law Offices), 09/05/2022. Available at: https://www.grandwaylaw.com/guofengshijiao/3716.html (Last Access: 15/05/2023)

Quanguo Fayuan Xitong 2022 Niandu Youxiu Anli Fenxi Pingxuan Huojiang Mingdan 全国法院系统 2022 年度优秀案例分析评选获奖名单 (National Court System 2022 Excellent Case Analysis Award Winner List). Available at: https://www.163.com/dy/article/HPU7DGMV051486CM.html (Last Access: 03/05/2023)

Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), 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 People's Republic of China), 20/08/2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), Zhonghua Renmin Gongheguo Xingzheng Chufa Fa 中华人民共和国行政处罚法 (Administrative Punishments Law of the PRC) Available at: http://www.npc.gov.cn/npc/c30834/202101/49b50d96743946bda545ef0c333830b4.shtml

Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People's Congress of the People's Republic of China), Zhonghua Renmin Gongheguo Shuju Anquan Fa 中华人民共和国数据安全法 (The Data Security Law of the PRC), 10/06/2021. Available at: http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml

Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People-s Congress of the PRC), Zhonghua Renmin Gongheguo Minfa Dian 中华人民共和国民法典 (Chinese Civil Code), 02/06/2020. Available at: http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml

Quanguo Renmin Daibiao Dahui 全国人民代表大会 (The National People-s Congress of the PRC), Zhonghua Renmin Gongheguo Minfa Zongze 中华人民共和国民法总则 (General Principles of Civil Law), 15/03/2017. Available at: http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-03/15/content_2018907.htm

Quanguo Xinxi Anquan Biaozhunhua Jishu Weiyuanhui 全国信息安全标准化技术委员会 (National Information Security Standardization Technical Committee), *Wangluo Anquan Biaozhun Shijian Zhinan – Geren Xinxi Kua Jing Chuli Huodong Anquan Renzheng Guifan* 网络安全标准实践指南—个人信息跨境处理活动安全认证规范 (*the Network Security Standard Implementing Guidance – Certification Technical Specification for Cross-border Personal Information Transfers*), 16/12/2022. Available at: https://www.tc260.org.cn/upload/2022-12-16/1671179931039025340.pdf

Quanguo Xinxi Anquan Biaozhunhua Jishu Weiyuanhui 全国信息安全标准化技术委员会 (National Information Security Standardization Technical Committee), *Guanyu Guojia Biaozhun《Xinxi Anquan Jishu Geren Xinxi Kua Jing Chuanshu Renzheng Yaoqiu》*

Zhengqiu Yijian Gao Zhengqiu Yijian De Tongzhi 关于国家标准《信息安全技术 个人信息跨境传输认证要求》征求意见稿征求意见的通知 (*Notice on the national standard "Information Security Technology Personal Information Cross-border Transmission Authentication Requirements" draft for comments*), 16/03/2023. Available at: https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20230316143506&norm_id=20221102152946&recode_id=50381

Rochet, Jean-Charles, Tirole, Jean, *Platform Competition in Two-Sided Markets*, Journal of the European Economic Association, 1(1), 1990 June 2003, pp. 990–1029. https://doi.org/10.1162/154247603322493212

Shishang Zui Yan Shuju Baohu Fa An GDPR Zhengshi Shengxiao Chang Bi Guanxia Dianfu Ji You Shangye Moshi 史上最严数据保护法案 GDPR 正式生效 "长臂管辖" 颠覆既有商业模式 (The strictest data protection bill in history, GDPR, has come into force, and the "long arm jurisdiction" has disrupted the established business model.), Xinliang Caijing 新浪财经 (Sina), 02/06/2018. Available at: http://finance.sina.com.cn/roll/2018-06-02/doc-ihcikcew5084521.shtml (Last Access: 03/05/2023)

Skiera, Bernd, Miller, Klaus, Jin, Yuxi, Kraft, Lennart, Laub, Rene, Schmitt, Julia, *The impact of the general data protection regulation (GDPR) on the online advertising market*, Self-Publishing, 2022.

Sun, Yuchuan, *Legal Compliance of Workplace Surveillance in China -From a Personal Information Protection Perspective*, China Legal Newsletter, Hanling&Partners, July 2022. Available at: https://www.ohebashi.com/jp/newsletter/CN_NL_EN_Vol.2_Yuchuan%20Sun.pdf (Last Access: 15/05/2023)

Sun, Yuchuan, *Legal Compliance of Workplace Surveillance in China -From a Personal Information Protection Perspective*, China Legal Newsletter, Hanling&Partners, July 2022. Available at: https://www.ohebashi.com/jp/newsletter/CN_NL_EN_Vol.2_Yuchuan%20Sun.pdf (Last Access: 15/05/2023)

The GDPR: Extending The Long Arm Of The Law, Hong Kong Lawyer, 07/2018. Available at: https://www.hk-lawyer.org/content/gdpr-extending-long-arm-law (Last Access: 27/04/2023)

Wang, Chunhui 王春晖, *"Gerenxinxi Baohufa" de Shida Hexin Yaodian Jiexi*《个人信息保护法》的十大核心要点解析 *(Analysis of the Ten Core Points of the Personal Information Protection Law.*), Zhongguo Dianxin Ye 中国电信业 (China Telecom Industry), 1 (2022): 54-60.

Wang, Echo, Sen, Anirban, Murdoch Scott, *China's Didi raises $4.4 bln in upsized U.S. IPO*, Reuters, 20/06/2021. Available at: https://www.reuters.com/business/chinas-didi-raises-4-billion-us-ipo-source-2021-06-29/ (Last Access: 03/04/2023)

Wang, Yuan, 王苑, *Shuju Quanli Shiye Xia Geren Xinxi Baohu De Quxiang – Yi Gerenxinxibaohu Yu Yinsiquan De Fenli Wei Zhongxin* 数据权力视野下个人信息保护的趋向 ——— 以个人信息保护与隐私权的分立为中心 (*The Trend of Personal Information Protection from the Perspective of Data Power: Centered on the Separation of Personal Information Protection and Privacy Rights*.), Beijing Hangkong Hangtian Daxue Xuebao (Shehui Kexue Ban) 北京航空航天大学学报 (社会科学版) (Journal of Beihang University, Social Science Edition), 35.1 (2022): 45-57.

Weinaicai Yu Hengtong Xiangjiao Zhipin (Shenzhen) Youxian Gongsi Laodong Zhengyi Ershen Minshi Panjueshu 韦乃财与恒通橡胶制品（深圳）有限公司劳动争议二审民事判决书 (Civil Judgment of Second Instance of Labor Dispute between Wei Naicai and Hengtong Rubber Products (Shenzhen) Co., Ltd.), 29/12/2014. Available at: https://aiqicha.baidu.com/wenshu?wenshuId=29660a4cff4ff18f63c4576f7e9511fc888d38d5

What is Data Mapping?, Talend. Available at: https://www.talend.com/resources/data-mapping/

Wo Guo de Laodong Falu Zhidu 我国的劳动法律制度 (China's labor law system), Shi jie Quanguo Renda Changwei Hui Fazhi Jiangzuo Di Shiba Jiang 十届全国人大常委会法制讲座第十八讲 (The 18th lecture on the legal system of the Standing Committee of the 10th National People's Congress). Available at: http://www.npc.gov.cn/zgrdw/npc/xinwen/2006-03/21/content_347935.htm (Last Access: 29/04/2023)

Wu Zhongjun, Shenzhenshi Tengruifeng Keji Youxian Gongsi Laodong Hetong Jiufen Ershen Minshi Panjueshu 吴仲军、深圳市腾瑞丰科技有限公司劳动合同纠纷二审民事判决书 (Wu Zhongjun, Shenzhen Tengruifeng Technology Co., Ltd. labor contract dispute second instance civil judgment), 30/06/2019. Available at: https://aiqicha.baidu.com/wenshu?wenshuId=f6849347470bda83ca78e96fc22a59009a7d502f

Xinxi Anquan Jishu Gonggong Ji Shangyong Fuwu Xinxi Xitong Geren Xinxi Baohu Zhinan 信息安全技术公共及商用服务信息系统·个人信息保护指南 (Information Security Technology Guidelines for Personal Information Protection on Public and Commercial Service Information Systems), 21/01/2013. Available at: https://digichina.stanford.edu/work/information-security-technology-guidelines-for-personal-information-protection-on-public-and-commercial-service-information-systems/

Xu, Manjing, Wang, Dongxu, Peng, Beisen, 许蔓菁, 王东旭, 彭焙森, *Geren Xinxi Baohufa Shishi Xia de Shuzi Yingxiao Fazhan Tantao*《个人信息保护法》实施下的数字营销发展探讨 (*Discussion on the development of digital marketing under the implementation of "Personal Information Protection Law"*), Xiandai Shangye 现代商业 (Modern Business Magazine) 2023, No.663(02): 32-35. Available at: https://www.xdsyzzs.com/zixun/7920.html

Xu, Mingjiao 徐明皎, *Geren Xinxi Quanmian Baohu Shidai Shuzihua Yingxiao Yinglai Biange* 个人信息全面保护时代 数字化营销迎来变革 (*In the era of comprehensive protection of personal information, digital marketing ushered in changes*), Fazhiwang 法治网 (Legal daily), 7/12/2021. Available at: http://www.legaldaily.com.cn/zt/content/2021-12/07/content_8640081.htm (Last Access: 21/04/2023)

Xue, Janet Hui, *Delegitimising Data Subjects' Economic Interests During Automatic Propertisation of Their Data: A Comparative Study of Data Protection on Social Media Platforms in the UK and China*, Global Media and China, 7(2), 151–168, 2022. https://doi.org/10.1177/20594364211060874

Yan Luo, Rui Guo, F*acial Recognition in China: Current Status, Comparative Approach and the Road Ahead*, 25 U. Pa. J.L. & Soc. Change 153 (2022). Available at: https://scholarship.law.upenn.edu/jlasc/vol25/iss2/3 https://doi.org/10.1016/B978-0-12-815300-0.00007-1

Yan Luo, Xuezi Dan, Christopher Adams, Sean Stein, *China Reveals Plan to Establish a National Data Bureau*, Global Policy Watch, Covington, 8/03/2023. Available at: https://www.globalpolicywatch.com/2023/03/china-reveals-plan-to-establish-a-national-data-bureau/ (Last Access: 22/03/2023)

Yongren danwei Shanzi Huifu de Yuangong Weixin Liaotian Jilu Nengfou Zuowei Shuju 用人单位擅自恢复的员工微信聊天记录能否作为证据？ (Can the employees' Wechat chat records restored by the employers without authorization be used as evidence?), Mingli Zhian 明理之案, 24/03/2023. Available at: https://baijiahao.baidu.com/s?id=1761248862658232832 (Last Access: 26/04/2023)

Yuangong Xingwei Jiance Jiufen Anli: Qiye Liyong Ruanjian Jiankong Yuangong Diannao Shuyu Ziwo Guanli Hangwei, Bu Qinfan Yuangong Yinsiquan 员工行为监测纠纷案例：企业利用软件监控员工电脑属于自我管理行为，不侵犯员工隐私权 (Employee Behavior Monitoring Dispute Case: The use of software by an enterprise to monitor employees' computers is self-management and does not infringe upon employees' right to privacy), 23/02/2023. Available at: https://mp.weixin.qq.com/s?__biz=MzI5Nzc5MTI3MQ==&mid=2247513001&idx=1&sn=49d6fb054bd53717503e57ec5abcbee7&chksm=ecad49e1dbdac0f7309942b6f2d0511f96c21d4d2acee7cd4a05d01ba27bde848f705bff2b05&scene=27

Zeng, Shihong, Ya Zhou, *Foreign Direct Investment's Impact on China's Economic Growth*, Technological Innovation and Pollution., International journal of environmental research and public health vol. 18,6 2839. 10 Mar. 2021, doi:10.3390/ijerph18062839

Zhang, Fanny, Zhou Qian, *China's New Personal Information Protection Law: Impact on Employment Management*, China Briefing, 23/09/2021. Available at: https://www.china-briefing.com/news/chinas-new-personal-information-protection-law-impact-on-employment-management/ (Last Access: 03/05/2023)

Zhang, Justina, *China's PI Certification for Cross-border Data Transfer: What You Need to Know*, GALA, 31/03/2023. Available at: http://blog.galalaw.com/post/102ibr9/chinas-pi-certification-for-cross-border-data-transfer-what-you-need-to-know (Last Access: 09/05/2023)

Zhang, Lu, *Personal information of privacy nature under Chinese Civil Code*, Computer Law & Security Review, Volume 43, 2021, 105637, ISSN 0267-3649. Available at: https://doi.org/10.1016/j.clsr.2021.105637

Zhang, Thomas, *GDPR Versus PIPL – Key Differences and Implications for Compliance in China*, China Briefing, 18/05/2022. Available at: https://www.china-briefing.com/news/pipl-vs-gdpr-key-differences-and-implications-for-compliance-in-china/ (Last Access: 22/03/2023)

Zhang, Thomas, *Personal Information Protection Law in China: Technical Considerations for Companies*, China Briefing, 23/08/2021. Available at: https://www.china-briefing.com/news/personal-information-protection-law-in-china-technical-considerations-for-companies/ (Last Access: 25/03/2023)

Zhang, Thomas, *Personal Information Protection Law in China: Technical Considerations for Companies*, China Briefing, 8, 23, 2021. Available at: https://www.china-briefing.com/news/personal-information-protection-law-in-china-technical-considerations-for-companies/ (Last Access: 12/05/2023)

Zhang, Thomas, *PIPL China: Suggestions for Technical Compliance with Personal Information Protection Law*, China Briefing, 25/10/2021. Available at: https://www.china-briefing.com/news/pipl-china-suggestions-on-technical-measures-for-compliance/ (Last Access: 11/04/2023)

Zhang, Zhenxing, Zha, Yunfei, *The Systematic Construction of Lawfulness of Processing Employees' Personal Information Under the Chinese Personal Information Law*, 13/09/2022. Available at: http://dx.doi.org/10.2139/ssrn.4218180

Zhao Xinhua, Wang Zhefeng, ShanWenyu 赵新华, 王哲峰, 单文钰, *Kuaguo Qiye Shuju Anquan Shijian de Yufang Yu Yingdui (Shangpian) – Fang Zhi Yu Wei Meng, Zhizhi yu Wei Luan* 跨国企业数据安全事件的预防与应对（上篇）——防之于未萌，治之于未乱 *(Prevention and Response to Data Security Incidents of Multinational Enterprises (Part 1) — Preventing the Unseen and Treating the Unsettled*), Jindu Lushi Shiwu Suo 金杜律师事务所 (King&Wood Mallesons), 03/03/2023. Available at: https://www.kwm.com/cn/zh/insights/latest-thinking/prevention-of-data-security-incidents-for-multinational-enterprises.html (Last Access: 19/03/2023)

Zheng, Guan, *Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S. and China*, Computer Law & Security Review, Volume 43, 2021, 105610, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2021.105610

Zhong, Xin 钟新, *Waizi Qiye Hegui Guanli Shuju Anquan* 外资企业合规管理之数据安全 *(Data Security for Compliance Management of Foreign-funded Enterprises)*, Guohao Lushi Shiwu Suo 国浩律师事务所 (Grandall Law Firm), 28/07/2021. Available at: https://www.grandall.com.cn/ghsd/info_17.aspx?itemid=23984 (Last Access 08/04/2023)

Zhongguo Zhongxiao Qiye Guoji Hezuo Xiehui, Guanyu Xiehui 中国中小企业国际合作协会，关于协会, (China International Cooperation Association of SME, About us). Available at: https://xiehui.chinasme.org.cn/site/content/7373.html (Last Access: 02/04/2023)

Zhonghua Renmin Gongheguo Guojia Hulianwang Xinxi Bangongshi 中华人民共和国国家互联网信息办公室 (Cybespace Administration of China), *Shuju Chujing Anquan Pinggu Banfa* 数据出境安全评估办法 (*Outbound Data Transfer Security Assessment Measures*), 07/07/2022. Available at: http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm

Zhonghua Renmin Gongheguo Guojia Hulianwang Xinxi Bangongshi 中华人民共和国国家互联网信息办公室 (Cybespace Administration of China), *Shuju Chujing Anquan Pinggu Banfa* 数据出境安全评估办法 (*Outbound Data Transfer Security Assessment Measures*), 07/07/2022. Available at: http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm

Zhonghua Renmin Gongheguo Guojia Hulianwang Xinxi Bangongshi 中华人民共和国国家互联网信息办公室 (Cyberspace Administration of China), *Geren Xinxi Baohu Renzheng Shishi Guize* 个人信息保护认证实施规则 (*Implementation Rules for Personal Information Protection Certification*), 18/11/2022. Available at: http://www.cac.gov.cn/2022-11/18/c_1670399936983876.htm

Zhonghua Renmin Gongheguo Guojia Hulianwang Xinxi Bangongshi 中华人民共和国国家互联网信息办公室 (Cybespace Administration of China), *Geren Xinxi Chujing Biaozhun Hetong Banfa* 个人信息出境标准合同办法 (*Standard Contract Measures for the Export of Personal Information*), 22/02/2023. Available at: http://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm

Zhonghua Renmin Gongheguo Guowuyuan Ling 中华人民共和国国务院令，第 700 号 (Decree of the State Council of the PRC, n. 700), Renli Ziyuan Shichang Zanxing Tiaoli 人力资源市场暂行条例 (Interim Regulation on Human Resources Market). Full text available at: http://www.gov.cn/zhengce/content/2018-07/17/content_5306967.htm

Zhonghua Renmin Gongheguo Hulianwang Xinxi Bangongshi 中华人民共和国国家互联网信息办公室 (The Cyberspace Administration of China), *Guojia Hulianwang Xinxi Bangongshi Dui Didi Quanqiu Gufen Youxian Gongsi Yifa Zuochu Wangluo Anquan Shencha Xiangguan Xingzheng Chufa de Jueding* 国家互联网信息办公室对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定 (*The Cyberspace Administration of China has made a decision on administrative punishment related to network security review against Didi Global Co., Ltd*. Available at: http://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm (Last Access: (05/04/2023)

Zhonghua Renmin Gongheguo Hulianwang Xinxi Bangongshi 中华人民共和国国家互联网信息办公室 (The Cyberspace Administration of China), Zhonghua Renmin Gongheguo Wangluo Anquan Fa 中华人民共和国网络安全法 (The Cybersecurity Law of the PRC), 07/11/2016. Available at: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

Zhonghua Renmin Gongheguo Minfadian 中华人民共和国民法典 (Civil Code of the People's Republic of China), 28/05/2020. http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml

Zhonghua Renmin Gongheguo Zhongyang Renmin Zhengfu (Central People's Government of the People's Republic of China 中华人民共和国中央人民政府, Quanguo Renda Changwei Hui Guanyu Jiaqiang Wangluo Xinxi Baohu De Jueding 全国人大常委会关于加强网络信息保护的决定 (National People's Congress Standing Committee Decision concerning Strengthening Network Information Protection), 28/12/2012. Available at: http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm

Zhonghua Renmin Gongheguo Zhongyang Renmin Zhengfu 中华人民共和国中央人民政府 (The Central People's Government of the PRC), *Zhonghua Renmin Gongheguo Laodongfa* 中华人民共和国劳动法 (*Labor Law of the PRC*), 05/07/1994. Available at: http://www.gov.cn/banshi/2005-05/25/content_905.htm

Zhonghua Renmin Gongheguo Zhongyang Renmin Zhengfu 中华人民共和国中央人民政府 (Central People's Government of the People's Republic of China), Guowuyuan Guanyu Yinfa Shehui Xinyong Tixi Jianshe Guihua Gangyao (2014-2020 Nian) de Tongzhi 国务院关于印发社会信用体系建设 规划纲要 (2014—2020 年）的通知 (The State Council on the issuance of the social credit system construction. Notice of Planning Outline (2014-2020), 27/06/2014. Available at: http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm

Zhonghua Renmin GongheGuo Zhongyang Renmin Zhengfu 中华人民共和国中央人民政府 (The Central People's Government of the People's Republic of China), *Zhonghua Renmin Gingheguo Laodong Hetong Fa* 中华人民共和国劳动合同法 (*Labor Contract Law of the People's Republic of China*). Available at: http://www.gov.cn/flfg/2007-06/29/content_669394.htm

Zhonghua Renmin Gongheguo Zhongyang Renmin Zhengfu 中华人民共和国中央人民政府 (Central People's Government of the People's Republic of China), Guojia Fazhan Gaige Wei Guanyu Yinfa "Shisiwu Tuijin Guojia Zhengwu Xinxihua Guihua" de Tongzhi 国家发展改革委关于印发《"十四五"推进国家政务信息化规划》的通知 (Notice of the National Development and Reform Commission on Printing and Distributing the "14th Five-Year Plan for Promoting National Government Informationization"), 2021. Available at: http://www.gov.cn/zhengce/zhengceku/2022-01/06/content_5666746.htm

Zhonghua Renmin Gongheguo Zhongyang Renmin Zhengfu 中华人民共和国中央人民政府 (Central People's Government of the People's Republic of China), Guifan Hulianwang Xinxi Fuwu Shichang Zhixu Ruogan Guiding 规范互联网信息服务市场秩序若干规定 (Some Provisions to Standardize Internet Information Service Market Order), 29/12/2011. Available at: http://www.gov.cn/gongbao/content/2012/content_2161726.htm

Zhonghua Renmin Gongheguo Zhongyang Renmin Zhengfu 中华人民共和国中央人民政府 (Central People's Government of the People's Republic of China), Zhonghua Renmin Gongheguo Wangluo Anquanfa 中华人民共和国网络安全法 (The Cybersecurity Law of the PRC), 07/11/2016. Available at: http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm

Zhonghua Renmin Gongheguo Zuigao Renmin Fayuan 中华人民共和国最高人民法院 (The Supreme People's Court of the PRC), Guanyu Shenli Shiyong Ren Lian Shibie Jishu Chuli Geren Xinxi Xiangguan Minshi Anjian Shiyong Falu Ruogan Wenti De Guiding 关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定 (Provisions on Several Issues Concerning the Application of Law in the Trial of Civil Cases Related to the Use of Face Recognition Technology to Handle Personal Information), 28/07/2021. Available at: https://www.court.gov.cn/fabu-xiangqing-315851.html

Zhonghua Renmin Gonheguo Guoyuan Ling 中华人民共和国国务院令, 第 535 号 (Decree of the State Council of the PRC, n. 535), *Zhonghua Renmin Gongheguo Laodong Hetongfa Shishi Tiaoli* 中华人民共和国劳动合同法实施条例 (*Implementation Regulations for the PRC Labor Contract Law*), 18/09/2008. Available at: http://www.gov.cn/zwgk/2008-09/19/content_1099470.htm

Zhu, Yingying, *Personal Data Breach Incident Notification under the PIPL, Mingdun Law Firm*, 16/03/2022. Available at: http://en.mdlaw.cn/news_view.aspx?TypeId=5&Id=403&Fid=t2:5:2 (Last Access: 25/03/2023)