EJLT European Journal of Law and Technology

Processing of Personal Data by Public Authorities in China: Assessing Equivalence for Cross-border Transfers from the EU to China

Yueming Zhang*

Abstract

The *Schrems II* judgement highlights that how the foreign public authorities access and process personal data has become an important factor in determining whether EU citizens' personal data can be transferred to a third country. In China, on the one hand, the Personal Information Protection Law (PIPL) sets out a series of provisions in relation to the processing of personal information by public authorities. On the other hand, several laws and regulations authorise public authorities to access personal information for national security and criminal law enforcement purposes. This paper analyses and examines the laws and practices in China regarding public authorities' access and use of personal data in light of the post-*Schrems II* data transfer standards.

* Yueming Zhang, PhD candidate, Ghent University, Research Group Law & Technology, Belgium, yueming.zhang@ugent.be

1. Introduction

Public authorities of a state, in general, can potentially collect and use massive amounts of personal data for different applications, in connection with their regulatory, security, law enforcement and social welfare tasks.[1] From a European data protection perspective, government access and use of personal data in a third country cannot be ignored in cases of cross-border data transfers.[2] The *Schrems II* decision[3] highlights that whether and how foreign public authorities have access to personal data is a factor that plays an important role in the assessment of whether personal data of EU citizens can be transferred to a third country.[4] As a result, companies which choose to maintain their transfers of personal data from the EU to China are required to assess the laws and practices regarding government access and use of personal data by the Chinese public authorities.[5]

The EU has paid much attention to the EU-US international data transfers. The *Schrems*[6] and *Schrems II* judgements are cornerstones which dealt with the transfer of personal data from the EU to the US and invalidated the adequacy decisions regarding to such transfers. Following the *Schrems II* judgement, the EU has launched the process to adopt an adequacy decision for the new EU-U.S. Data Privacy Framework.[7] However, the EU seems to pay less attention to China regarding data transfers. According to UNCTAD, the United States and China are the two countries that stand out in terms of their capacity to engage in and benefit from the data-driven economy.[8] Moreover, China is an important trade partner for the EU.[9] In this context, more legal certainty between the EU and China is urgently needed.

---

[1] Jamie P Horsley, 'How Will China's Privacy Law Apply to the Chinese State?' (*New America*, 26 January 2021) <http://newamerica.org/cybersecurity-initiative/digichina/blog/how-will-chinas-privacy-law-apply-to-the-chinese-state/> accessed 4 March 2022.

[2] Marc Rotenberg, 'Schrems II, from Snowden to China: Toward a New Alignment on Transatlantic Data Protection' (2020) 26 European Law Journal 141.

[3] *Case C-311/18 Data Protection Commissioner v Facebook Ireland and Schrems* [2020] EU:C:2020:559. ('*Schrems II*')

[4] Mark Nottingham, 'Applying the European Essential Guarantees to ASIO Computer Access Warrants: Can Australia Avoid the Trade Impact of Schrems II?' (Social Science Research Network 2021) SSRN Scholarly Paper ID 3933661 <https://papers.ssrn.com/abstract=3933661> accessed 18 December 2021.

[5] European Data Protection Board, 'Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures' (10 November 2020).

[6] *Case C-362/14 Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650. ('*Schrems*')

[7] 'Questions & Answers: EU-U.S. Data Privacy Framework, draft adequacy decision' (*The European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632> accessed 13 February 2023.

[8] UNCTAD, *Digital Economy Report 2021* (2021) <https://unctad.org/system/files/official-document/der2021_en.pdf> accessed 9 August 2022.

[9] 'EU Trade Relations with China' (*The European Commission*) <https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/china_en> accessed 4 September 2022.

This article examines the law and practices in China concerning government access to personal data, in order to assess whether it complies with the standards that the EU requires for cross-border data transfers. More specifically, Section 2 of this paper briefly explains the EU's standards for cross border data transfers post-*Schrems II*, with regard to foreign government access to personal data. Section 3 of this paper discusses how the Chinese data protection law applies to public authorities' processing of personal data. Third, Section 4 and Section 5 of this paper map and examine the relevant laws and regulations authorising and regulating public authorities' access personal information for national security and criminal law enforcement purposes in China. Section 6 evaluates the identified Chinese legal instruments in light of the EU's standards.

Taking into account the fact that the EU and Chinese legal frameworks are driven by a different legal culture and different overall purposes and legislative techniques, this paper aims to contribute to the current public debate regarding the legal uncertainty of cross-border data transfers from the EU to China.

2. The EU data protection framework for cross-border transfers and the European Essential Guarantees

From a European data protection perspective, the protection of personal data, including in the context of surveillance activities by States, is considered a 'fundamental human right' enshrined in Articles 7, 8 and 52 of the EU Charter of Fundamental Rights and Article 8 of the European Convention on Human Rights. [10] The high level of protection must also be guaranteed when personal data is transferred outside the EEA to a third country. As a result, the access to and use of personal data by third country governments has become an important element in the impact assessment of data transfers.[11] Under EU law, the General Data Protection Regulation (GDPR) [12] is one of the important cornerstones of the secondary legislation on data protection at EU level.[13] According to Chapter V of the GDPR, data transfers to third countries may take place if the third country ensures an adequate level of protection

[10] European Data Protection Board (n 5) para 2.

[11] Barbara Sandfuchs, 'The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II' (2021) 70 GRUR International 245; Marcelo Corrales Compagnucci, Mateo Aboy and Timo Minssen, 'Cross-Border Transfers of Personal Data After Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)' (2021) 4 Nordic Journal of European Law 37.

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.

[13] Other legislative instruments are the Law Enforcement Directive (LED) which provides rules specifically with regard to the processing of personal data by 'competent authorities' for the purposes of 'the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties' (Article 1 LED) and the e-Privacy Directive, which has been under review for many years.

based on 'adequacy decisions' issued by the European Commission, or if the data controller or processor provides 'appropriate safeguards'.[14]

With regard to the criteria for obtaining an 'adequacy decision', the *Schrems* judgement has made it clear that the level of protection of personal data provided the third country should be 'essentially equivalent' to that guaranteed EU.[15] This option is not relevant to EU-China data transfers since there currently is no adequacy decision for China.[16] With regard to the 'appropriate safeguards', the *Schrems II* judgement highlights that 'essentially equivalent' level of protection also applies to appropriate safeguards.[17] The CJEU thus makes it clear that the concept of '*essential equivalence*' establishes a standard for cross border data transfers.[18] One element to understand the European standard is the European Essential Guarantees (EEG),[19] which provide the basis for state surveillance measures in a third country to be considered adequate. The EDPB has made it clear that these standards are relevant to the protection of fundamental human rights referred to in the Charter, and must be interpreted in light of the CJEU and ECtHR case law regarding state surveillance measures.[20] The European Essential Guarantees outline four guarantees for government access and use of personal data in a third country's law and practice: [21]

The first guarantee requires that processing should be based on clear, precise and accessible rules. It means that the applicable law should indicate clearly and precisely 'in which circumstances and under which conditions a measure providing for the

[14] In the absence of either of the ways, a number of derogations are available. However, the transfers based on derogations must be occasional and non-repetitive. See Article 49 of the GDPR.
[15] *Schrems* (n 6), para 73.
[16] See the website of the European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[17] *Schrems II* (n 3), para 92, emphasis added by the author. See, Zuzanna Gulczyńska, 'A Certain Standard of Protection for International Transfers of Personal Data under the GDPR' (2021) 11 International Data Privacy Law 360.
[18] Christopher Kuner, 'Schrems II Re-Examined' (*Verfassungsblog*, 25 August 2020) <https://verfassungsblog.de/schrems-ii-re-examined/> accessed 1 March 2021.
[19] The EES were drafted by the Article 29WP following the *Schrems I* judgment in order to understand which conditions need to be fulfilled in order for state surveillance measures in a third country to be considered 'adequate'. See, Article 29 Working Party, 'Working Document 01/2016 on the Justification of Interferences with the Fundamental Rights to Privacy and Data Protection through Surveillance Measures When Transferring Personal Data (European Essential Guarantees): WP 237' (13 April 2016). This document was modified by the European Data Protection Board, in order to add new elements following the *Schrems II* judgement, See European Data Protection Board (n 5).
[20] Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222; European Data Protection Board (n 5).
[21] European Data Protection Board (n 5) para 24.

processing of personal data may be adopted'.[22] The applicable law must also define 'the scope of the limitation on the exercise of the right concerned'.[23]

The second guarantee requires that 'the necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated'. This guarantee entails that a limitation on the rights to data protection may only be justified through the balance test between the seriousness of the interference and the importance of the public interest objective.[24] It also requires that the law must establish 'a connection between the data retained and the objective pursued'.[25]

The third guarantee requires that any interference should be subject to an independent oversight mechanism. This guarantee demands that the oversight body must be 'sufficiently independent from the executive institutions and the authorities carrying out the surveillance'.[26]

Fourth, effective remedies need to be available to the individual. This guarantee requires that the individual should be notified once the surveillance is over.[27] This guarantee also entails that individuals must have the right to bring legal action before an independent tribunal in order to exercise their data subject rights.[28]

Importantly, both the CJEU and the European Commission have made it clear in the *Schrems* cases and in existing adequacy decisions that it is essential to assess, in addition to the third country's data protection law, the third country legislation '*concerning public security, defence, national security and criminal law and the access of public authorities to personal data*'. This article uses the European Essential Guarantees as a framework to evaluate the relevant Chinese laws identified in the following sections.

3. The data protection framework for processing of personal data by public authorities in China

First of all, Article 33 of the Chinese Constitution provides that '*every citizen shall enjoy the rights prescribed by the Constitution and the law*'.[29] The Chinese Constitution protects the right to freedom and confidentiality of correspondence[30] and privacy of the home,[31] but does not include a general and more encompassing right to privacy. When necessary, '*to meet the needs of national security or of criminal investigation",*

[22] Ibid., 28.
[23] Ibid., 29, quoting *Schrems II* para 175.
[24] Ibid., 33, quoting *La Quadrature du Net and others*, para 131.
[25] Ibid., 38, quoting *Schrems II* para 180.
[26] Ibid., 42, quoting *Zakharov* para 281.
[27] Ibid., 45, quoting *Kennedy* para 190.
[28] Ibid., 48.
[29] Article 33 (4) Constitution of China.
[30] Article 40 Constitution of China.
[31] Article 39 Constitution of China.

"public security or procuratorate organs are permitted to censor correspondence in accordance with the procedures prescribed by law'.[32]

In principle, all 'state organs' and 'public authorities' in China must abide by the Constitution and the law.[33] In this regard, the Chinese Civil Code requires state organs and public authorities to keep the information they learn while performing their duties confidential and not leak it or unlawfully provide it to others.[34] The Constitution also protects the right of citizens to obtain compensation for infringements by state organs and their personnel.[35]

China did not have a comprehensive data protection framework until recently. China's efforts on regulating data protection issues started in 2012, marked by the *Decision on Strengthening Network Information Protection promulgated by the Standing Committee of the National People's Congress*.[36] The Cybersecurity Law (CSL) was introduced in 2016, which included the most comprehensive data protection principles at that point.[37] The CSL has a broader scope than the previous laws and brings China closer to global standards.[38] The efforts to protect personal information were also reflected in the Civil Code and Criminal Law in China. The Civil Law of China protects natural persons' right to privacy and personal information. The Civil Code also involves the basic data processing principles of 'lawfulness, justification and necessity'.[39] In 2015, the Ninth Amendment to China's Criminal Law introduced the crime of 'infringing personal information'.[40] Eventually, multiple regulations in relation to the protection of personal data could be found in both public and private law, such as the E-commerce Law and the Consumer Protection Law. These fragmented rules and regulations added up to a 'data protection cumulative effect' applicable to the private sector, meaning a certain point in time the personal information processing is in one way or another regulated.

This changed on 20 August 2021, when China passed its first comprehensive data protection law. The Personal Information Protection Law (PIPL) supplements the abovementioned instruments[41] and represents a crucial pillar in China's efforts to

---

[32] Article 40 Constitution of China.
[33] Article 5 Constitution of China.
[34] Article 1039 of the Civil Code of China.
[35] Article 41 Constitution of China.
[36] Decision on Strengthening Network Information Protection promulgated by the Standing Committee of the National People's Congress (全国人大常委会关于加强网络信息保护的决定) <http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm> accessed 18 August 2022.
[37] Graham Greenleaf and Scott Livingston, 'China's New Cybersecurity Law – Also a Data Privacy Law?' (Social Science Research Network 2016) SSRN Scholarly Paper ID 2958658 <https://papers.ssrn.com/abstract=2958658> accessed 29 January 2020.
[38] Emmanuel Pernot-LePlay, 'China's Approach on Data Privacy Law: A Third Way between the U.S. and the E.U.?' (2020) 8 Penn State Journal of Law & International Affairs 49.
[39] Article 1032 and 1034 of the Chinese Civil Code.
[40] Article 253(1) of China's Criminal Law.
[41] Todd Liao and others, 'Personal Information Protection Law: China's GDPR Is Coming' (*Morgan Lewis*, 24 August 2021) <https://www.morganlewis.com/pubs/2021/08/personal-information-protection-law-chinas-gdpr-is-coming> accessed 8 October 2021. As the main law for protecting

regulate the access to and use of personal data.[42] Having come into force since 1 November 2021, the PIPL is modelled at least in part on other data protection regimes like the GDPR.[43] Almost meanwhile, the Data Security Law (DSL) was adopted as another pillar of the broader Chinese data protection framework. The DSL forms the cornerstone of the protection of security of data in order to protect the national security and the public security, covering both personal data and non-personal data.[44]

With regard to government access to personal data, there were no restrictions in data protection regulations on the government's power to request companies to provide access to personal information before the PIPL was enacted.[45] Criticism was expressed when assessing the data protection rights in the relation between citizens and the government.[46] The CSL itself provides an example of this dichotomy. The CSL is applicable to private actors, namely 'network operators', and creates various obligations for the network operators regarding the protection of personal information.[47] On the other hand, according to Article 28 of the CSL, network operators also have the obligation to provide '*support and assistance to public authorities' activities preserving national security and investigating crimes*'.[48]

The PIPL, however, is the first legal instrument in China constraining public authorities' activities regarding the processing of personal information. It specifically imposes personal information processing requirements on 'state organs'.[49] The notion 'state organs' in China refers to 'the institutions established by the State to carry out its functions of political domination and administration'.[50] The scope of 'state organs'

personal information, the new PIPL will replace articles from former legal instruments which conflict with it.

[42] Guan Zheng, 'Trilemma and Tripartition: The Regulatory Paradigms of Cross-Border Personal Data Transfer in the EU, the U.S. and China' (2021) 43 Computer Law & Security Review.

[43] European Data Protection Board, 'Legal Study on Government Access to Data in Third Countries' (2021) <https://edpb.europa.eu/our-work-tools/our-documents/legal-study-external-provider/legal-study-government-access-data-third_en> accessed 10 January 2022.

[44] Rogier Creemers, 'China's Emerging Data Protection Framework' (2022) 8 Journal of Cybersecurity tyac011.

[45] Pernot-LePlay (n 38).

[46] Qingbai Sun(孙清白), 'Special Risks and Legal Regulations of Government Agencies Dealing with Personal Information (国家机关处理个人信息的特殊风险及其法律规制)' (2022) 46 Journal of Anhui University (Philosophy and Social Science Edition)(安徽大学学报哲学社会科学版) 88; James Fry, 'Privacy, Predictability and Internet Surveillance in the U.S. and China: Better the Devil You Know?' (2015) 37 University of Pennsylvania Journal of International Law 419; Pernot-LePlay (n 38).

[47] Article 76 (3) of the CSL. 'Network operators' refers to network owners, managers and network service providers.

[48] Article 28 of the CSL.

[49] Article 33 PIPL.

[50] Xiao Cheng (程啸), *The Interpretation of Personal Information Protection Law of the People's Republic of China (个人信息保护法理解与适用)* (China Legal Publishing House (中国法制出版社有限公司) 2021); Weiqiu Long (龙卫球), *Interpretation of the Personal Information Protection Law of the People's Republic of China (中华人民共和国个人信息保护法释义)* (China Legal Publishing House (中国法制出版社有限公司) 2021).

includes the Communist Party Committees, the Courts, procuratorates as well as governments and their departments.[51] Furthermore, Article 37 specifies that the PIPL also applies to the authorities who are '*authorised by laws and regulations to manage public affairs in order to perform their statutory duties*'. These authorities will include, for instance, industry associations or companies when they are delegated by law or other regulations to conduct public and social affairs.[52] For instance, the Law on Prevention and Treatment of Infectious Diseases authorises disease prevention agencies and medical institutions to collect and report information regarding the spread of pandemics.[53] In principle, all of the public authorities in China have to comply with the PIPL.

3.1 Purposes, scope and limitations

The PIPL provides seven lawful bases for processing personal information. These grounds include six lawful bases and an exception mentioning 'other circumstances provided in laws and administrative regulations'.[54] When public authorities process personal information, they must also rely on at least one of these lawful bases or another lawful basis provided by a specific rule of law. The PIPL, however, fails to expressly explain how these lawful bases are applied to public authorities.[55] Overall, the lawful bases that public authorities can rely on include: the necessity for exercising legal duties, necessity for performing contracts, protecting citizens' rights under emergency circumstances, and reasonable processing of personal information that has already been voluntarily disclosed. Consent can also be used with limitations, as the power imbalances between individuals and public authorities might make the consent unlikely to be freely given.[56]

When public authorities process personal information, they in principle have to comply with the requirements of the PIPL. So far there is no separate law in China for processing of personal data for law enforcement purposes, unlike in the EU, where the Law Enforcement Directive provides for a separate framework. As a result, data processing activities for criminal law enforcement and national security purposes also have to comply with the obligations set by the PIPL when personal information is

[51] Leading Group of the Supreme People's Court for the Implementation of the Civil Code(最高人民法院民法典贯彻实施工作领导小组主编), *The Interpretation and Application of the General Provisions of the Civil Code of the People's Republic of China (中华人民共和国民法典总则编理解与适用),* People's Court Press (人民法院出版社) 2020.

[52] Cheng (程啸) (n 50).

[53] Law of the People's Republic of China on Prevention and Treatment of Infectious Diseases (中华人民共和国传染病防治法), unofficial translation: https://uk.practicallaw.thomsonreuters.com/w-010-8115?transitionType=Default&contextData=(sc.Default)&firstPage=true accessed 20 December 2022.

[54] Article 13 PIPL.

[55] Chun Peng (彭錞), 'On the Legal Basis for State Organs to Process Personal Data in China (论国家机关处理个人信息的合法性基础)' (2022) 01 Journal of Comparative Law (比较法研究) 1.

[56] ibid.

processed. This includes both the general requirements for all personal information handlers and specific provisions for public authorities.

Specifically, the PIPL stipulates the following limitations. On the one hand, the PIPL gives rise to a series of general data protection principles, including legality and necessity,[57] purpose limitation and data minimisation,[58] openness and transparency,[59] accuracy,[60] security[61] and data retention.[62] On the other hand, Chapter 2, Section 3 of the PIPL sets out three specific provisions related to the processing of personal information by public authorities.

First of all, the PIPL specifies that the processing of personal data by public authorities shall not exceed the scope necessary to carry out their responsibilities. They may process personal data only in accordance with the powers and procedures provided in laws or administrative regulations.[63] This principle reflects the EU's proportionality and necessity requirement and essentially mirrors Article 52 of the EU Charter.

Second, Article 35 of the PIPL specifies that public authorities shall fulfil the obligation to inform the data subject – as a reflection of the transparency requirement in the GDPR. However, this article further provides exceptions for the notification obligations where a provision in law or administrative regulation requires confidentiality or stipulates a notification exemption, or where the notification will hinder the public authorities from performing their duties. In the Chinese legislative framework, there are several laws that require confidentiality when processing personal information, such as the Counter-terrorism law[64] and the Counter-espionage Law.[65] In such circumstances, public authorities shall process personal information without notifying of the data subjects.

Third, Article 36 of the PIPL states that personal information 'processed by public authorities' shall be stored within the mainland territory of China, with strict conditions for data exports from China. The conditions include 'necessity' and a 'security assessment'.

Overall, the PIPL only provides general principles regarding the public authorities' obligations when they process personal information. These obligations, however, offer little clarity as to the actual interpretation and implementation for public

[57] Article 5 PIPL.
[58] Article 6 PIPL.
[59] Article 7 PIPL.
[60] Article 8 PIPL.
[61] Article 9 PIPL.
[62] Article 19 PIPL.
[63] Article 34 PIPL.
[64] The Counter-terrorism Law was adopted on 27 December 2015 and amended on 27 April 2018. The Counter-terrorism Law of the People's Republic of China (中华人民共和国反恐怖主义法) (*27 April 2018*) <https://www.chinalawtranslate.com/en/counter-terrorism-law-2015/> accessed 21 December 2022.
[65] The Counter-espionage Law of the People's Republic of China (中华人民共和国反间谍法) (*1 November 2014*) <https://www.chinalawtranslate.com/en/anti-espionage/> accessed 21 December 2022.

authorities. Scholars have argued that these rules need to be implemented by more detailed and enforceable rules.[66]

3.2 Oversight

The most important difference between the PIPL and the GDPR continues to be the absence of an independent data protection authority.[67] Under the PIPL, enforcement duties are shared by several administrations. Such 'supervisory authorities' include the State Internet Information Department (Cyberspace Administration of China, CAC) and the relevant State Council departments (such as the Ministry of Industry and Information Technology, MIIT), as well as relevant lower-level governments' departments.[68] These administrations, however, are subordinated to the central government or lower level governments, and cannot be deemed as 'independent' from the perspective of the GDPR.[69] The PIPL does not specifically mention which administration specifically oversee the public authorities.[70]

Suggestions for establishing a specialist data protection authority were made in the law-making process but not taken into account in the final draft.[71] Although the PIPL provides a specific list of the tasks and powers of these 'supervisory authorities', it is still not clear which authority has which power or task. The scope and limitations of the supervision powers are also not clear. The lack of clarification not only creates legal uncertainty in implementing the PIPL in China,[72] but will also be an obstacle for the Chinese data protection framework to be regarded as 'essentially equivalent' to the GDPR.

3.3 Data subject rights and redress mechanisms

The PIPL protects a number of data subject rights, including the the right to know and decide relating to their personal information, the right to access, the right to

---

[66] Sun(孙清白) (n 46).

[67] Graham Greenleaf, 'China Issues a Comprehensive Draft Data Privacy Law' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3795001 <https://papers.ssrn.com/abstract=3795001> accessed 21 December 2021.

[68] Article 60 PIPL.

[69] Anja Geller, 'How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective' (2020) 69 GRUR International 1191; Graham Greenleaf, 'China—From Warring States to Convergence?', *Asian Data Privacy Laws: Trade & Human Rights Perspectives* (Oxford University Press 2014) <https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780199679669.001.0001/acprof-9780199679669-chapter-7> accessed 3 February 2021.

[70] Sun(孙清白) (n 46); Hongzhen Jiang (蒋红珍), 'Administrative supervision in the Personal Information Protection law (《个人信息保护法》中的行政监管)' (2021) 05 China Law Review (中国法律评论) 48.

[71] Yehan Huang and Mingli Shi, 'Top Scholar Zhou Hanhua Illuminates 15+ Years of History Behind China's Personal Information Protection Law' (*DigiChina*) <https://digichina.stanford.edu/work/top-scholar-zhou-hanhua-illuminates-15-years-of-history-behind-chinas-personal-information-protection-law/> accessed 4 March 2022.

[72] Geller (n 69).

rectification, the right to deletion and the right to request an explanation.[73] Interestingly, there are no absolute exemptions for public authorities regarding these data subject rights. When public authorities process personal information, as a rule, these rights shall also apply. The Chinese legislative framework does provide remedies for individuals against the breach of data protection rights. In general, foreigners in China can enjoy data protection rights and remedies equal to Chinese citizens.[74]

The PIPL protects individuals' right to file a complaint in the event of unlawful processing of personal data. Furthermore, individuals can claim compensation for data privacy breaches. The compensation should cover the loss of the individuals or the benefit obtained by the personal information handlers.[75] If the personal information handlers violate the rights of a large amount of data subjects, it is possible for the Procuratorates or departments fulfilling personal information protection duties to bring a class-action suit with the Court.[76] Criminal law and administrative law procedures are also mentioned in the PIPL.[77] These rights, in principle, can be exercised against both private organisations as well as public authorities since there are no exceptions.

Overall, the PIPL provides various redress mechanisms to individuals, including both administrative-oriented mechanisms and possibilities for judicial remedies.

4. Access and use by public authorities for criminal law enforcement purposes

The Chinese Criminal Procedure Law was adopted on 1 July 1979, and has been amended three times.[78] The Criminal Procedure Law specifically authorises criminal investigation agencies to access personal information for criminal investigation and enforcement purposes, with a number of limitations.

4.1 Legal bases and scope

In general, for criminal investigation purposes, '*people's courts, people's procuratorates and public security organs have the right to gather and collect evidence from relevant workplaces and individuals in accordance with law*'[79]. The scope of

[73] Article 45-48 PIPL.
[74] See, Article 32 China's Constitution, Article 5 Civil Procedure Law and Article 395 Interpretations of the Supreme People's Court on the Application of the 'Criminal Procedure Law of the People's Republic of China. Bo Zhao and GP (Jeanne) Mifsud Bonnici, 'Protecting EU Citizens' Personal Data in China: A Reality or a Fantasy?' (2016) 24 International Journal of Law and Information Technology 128.
[75] Ibid.
[76] Article 66 PIPL draft.
[77] Article 67 PIPL draft.
[78] The Criminal Procedure Law of the People's Republic of China (中华人民共和国刑事诉讼法). An unofficial translation: <https://www.chinalawtranslate.com/criminal-procedure-law-2018/> accessed 18 August 2022.
[79] Article 54 Criminal Procedure Law.

evidence in China includes physical and documentary evidence as well as audio-visual materials. Electronic data is also regarded as an independent form of evidence since the 2012 amendment of the Criminal Procedure Law.[80]

With regard to the territorial scope of collection of electronic data evidence, investigators are authorised to only obtain access to electronic data online in computer information systems located in China as well as public available data stored abroad for use in criminal investigations.[81] For data stored abroad, access can only be obtained through criminal justice assistance requests to the foreign country under certain procedures according to the International Criminal Justice Assistance Law.[82]

According to Sections 5 and 6, Chapter 2 of Part II of the Criminal Procedure Law, criminal investigation agencies are authorised to collect and use personal information through carrying out a search and seizure procedure. [83] Organisations and citizens have the obligation to comply with requests from procuratorate or public security organs to '*hand over physical evidence, documentary evidence, audio-visual recordings or other evidence that might prove the suspect's guilt or innocence*'.[84]

Furthermore, electronic data evidence can also be collected by 'technical investigation measures', in the case of crimes that '*endanger national security, terrorist activities, mafia-type organisation crimes, major drug crimes, or other crimes that seriously endanger society, upon having completed strict approval procedures*'.[85] Such technical investigation measures include monitoring of records, location, place and

[80] Article 50 Criminal Procedure Law. See Fan Yang and Jiao Feng, 'Rules of Electronic Data in Criminal Cases in China' (2021) 64 International Journal of Law, Crime and Justice 100453.
[81] The Ministry of Public Security of China(中华人民共和国公安部), 'the Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases(公安机关办理刑事案件电子数据取证规则)' <http://gaj.cq.gov.cn/zslm_245/wlaqgl/flfg/201912/t20191221_2043591.html> accessed 18 August 2022. See, European Data Protection Board (n 43); Yang and Feng (n 80).
[82] International Criminal Justice Assistance Law of People's Republic of China (中华人民共和国国际刑事司法协助法) (26 October 2018) <http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-10/26/content_2064576.htm> accessed 18 August 2022.
[83] Zhizheng Wang, 'Systematic Government Access to Private-Sector Data in China', *Bulk Collection* (Oxford University Press 2017) <https://oxford.universitypressscholarship.com/10.1093/oso/9780190685515.001.0001/oso-9780190685515-chapter-11> accessed 17 March 2022; Yang and Feng (n 80).
[84] Article 137 Criminal Procedure Law.
[85] Article 150 Criminal Procedure Law.

correspondence.[86] Organisations and citizens have the obligation to cooperate with the technical investigative measures.[87]

In short, personal information deemed as electronic evidence can be collected and used by criminal investigation authorities in China. Although the basic framework has been established by the Criminal Procedure Law, the aforementioned provisions are rather ambiguous and not clear enough.[88] The scope of 'electronic evidence' is broad and the border is unclear.

4.2 Limitations and safeguards

First of all, the objectives of the Chinese Criminal Procedure Law include '*respect for and protection of human rights*' and to '*protect the personal rights, property rights, democratic rights and other rights of citizens*'.[89] This is a reflection of the Chinese Constitution.[90] The investigation agencies only have the obligation to keep personal information confidential.[91]

Searching of evidence, including electronic data, should be conducted on the basis of a *warrant*. However, the search warrants are obtained through internal approval procedures instead of a court, and they may not be required if an emergency occurs.[92] It has thus been argued that privacy rights are vulnerable in judicial practice.[93]

All in all, compared to the broad scope of personal information that criminal investigation agencies can collect, the safeguards for personal information are limited.[94] One reason might be that the data protection framework is just established, being a relatively independent and new legal framework in China. As scholars have already suggested, the Criminal Procedure framework also needs to implement the

[86] Article 264 of The Ministry of Public Security of China(中华人民共和国公安部), Provisions on the procedures of public security organs handling criminal cases (公安机关办理刑事案件程序规定). http://www.ww010.com/page237?article_id=461&pagenum=9 accessed 18 August 2022. See Zongzhi Long(龙宗智), 'Seeking a Balance between Effective Evidence and Guaranteeing Rights - A Review of the Electronic Data Evidence Provisions (寻求有效取证与保证权利的平衡——评"两高一部"电子数据证据规定)' (2016) 11 Law Science (法学) 7.

[87] Article 152 Criminal Procedure Law.

[88] Yang and Feng (n 80).

[89] Article 2 Criminal Procedure Law.

[90] Article 37 of the Chinese Constitution.

[91] Article 54 Criminal Procedure Law. Similar regulations can also be found in Article 64 and Article 152 of Criminal Procedure Law.

[92] Article 138 Criminal Procedure Law. Zhizheng Wang, 'Systematic Government Access to Private-Sector Data in China' (2015) 2 International Data Privacy Law 220.

[93] Yang and Feng (n 80).

[94] Mei Liu (刘玫) and Yunan Chen (陈雨楠), 'From Conflict to Integration: The Construction of Rules for the Protection of Citizens' Personal Information in Criminal Investigations (从冲突到融入：刑事侦查中公民个人信息保护的规则建构)' (2021) 05 Research on Rule of Law (法治研究) 34; Long(龙宗智) (n 86).

data protection principles, by means of adding relevant rules into the Chinese Criminal Procedure law and setting limitations to investigatory powers.[95]

4.3 Oversight of criminal investigation agencies

The Cyberspace Administration of China and other relevant departments are responsible for the oversight of the practices regarding personal information protection of criminal investigation agencies. However, it has been argued that the Cyberspace Administration may lack knowledge of criminal investigation procedures, and may not have enforceable powers against the criminal investigation agencies.[96]

With regard to the oversight mechanisms set by the Criminal Procedure Law, the criminal investigation procedure is subject to internal oversight, but no independent external oversight.[97] The search warrants are also obtained through internal approval procedures rather than from a court.

The absence of a special and independent oversight department for data processing conducted by criminal investigation agencies can be regarded as a weakness of the current Chinese framework.

4.4 Data subject rights and individual redress mechanisms

In principle, individuals have various data protection rights against public authorities, including criminal investigation authorities, as stipulated by the PIPL. However, it is questionable whether the rights can be effectively implemented against the criminal investigation authorities.[98]

The current Criminal Procedure law system of China does not explicitly provide suspects with a basis for a remedy against the public authorities during a criminal investigation.[99] According to the State Compensation Law,[100] individuals may obtain compensation for infringements during detection, prosecution, adjudication and administration of prison procedures caused by public authorities. However, the scope

[95] Xi Zheng (郑曦), 'Outline of the protection of personal information in criminal proceedings (刑事诉讼个人信息保护论纲)' (2021) 35 Contemporary Law Review (当代法学) 115.
[96] Lei Cheng (程雷), 'Covert surveillance and the protection of citizens' personal information in the context of big data (大数据背景下的秘密监控与公民个人信息保护)' (2021) 36 Legal Forum (法学论坛) 15.
[97] ibid.
[98] Xixin Wang (王锡锌), 'An Analytical Framework of Legitimacy of Personal Information Processing by Administrative Agencies (行政机关处理个人信息活动的合法性分析框架)' (2022) 03 Journal of Comparative Law (比较法研究) 92.
[99] Zhongyang Wang (王仲羊), 'Protection of the rights of personal information in criminal proceedings (刑事诉讼中个人信息的权利保护)' (2022) 03 Criminal Science (中国刑事法杂志) 155; Yang and Feng (n 80).
[100] Law of the People's Republic of China on State Compensation (中华人民共和国国家赔偿法) http://www.npc.gov.cn/zgrdw/huiyi/lfzt/gjpcfxzaca/2008-10/22/content_1454086.htm

of violation only covers the right to liberty or property, but is not related to the right to privacy and personal information.[101]

Similarly, individuals have the right to sue public authorities based on the Administrative Procedure Law.[102] Again, the scope only covers infringements of the right to liberty or property but does not include infringements of the right to privacy and data protection.[103]

In short, the current criminal procedure legal framework in China prioritises remedies regarding their rights to physical health and property rights, while overlooking privacy and data protection rights.[104] Meanwhile, the available remedies are limited to filing complaints with internal departments and do not include access to judicial remedies. These mechanisms may not be considered adequately constructed according to the EU standards.

5. Access and use by public authorities for national security purposes

Similar to many countries in the world, China has laws requiring or authorising public authorities' access to personal information for national security purposes.

The Chinese Ministry of State Security (MSS) was established in 1983. Since then, several policy documents and instructions have been adopted related to national security.[105] In 1993, the National Security Law was adopted, but it only referred to counter-espionage issues and was therefore far from comprehensive. As a result, the national security framework has long been criticised for not being transparent or adequate.[106]

This began to change in 2014, as president Xi Jinping emphasised the pursuit of a '*holistic approach to national security in order to carry out the national security work well in the new era*' during the first meeting of the National Security Commission of the CPC Central Committee.[107] On 1 July 2015, the new Chinese National Security Law was adopted.[108] The new National Security Law is the first comprehensive national

[101] Article 17 and 18 State Compensation Law.
[102] Administrative Procedure Law (中华人民共和国行政诉讼法), http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-06/29/content_2024894.htm accessed 18 August 2022.
[103] Article 12 of the Administrative Procedure Law.
[104] Cheng (程雷) (n 96).
[105] Yuanfu Pang (庞远福), 'On the National Security Law: Background, Significance and Features of its Development (论《国家安全法》：制定背景、意义及其特征)' (2019) 09 Decision-making and information (决策与信息) 47.
[106] ibid.
[107] 'Political Bureau Adopts National Security Strategy Outline (政治局会议通过《国家安全战略纲要》)' (*People's Daily (人民网)*) <http://politics.people.com.cn/n/2015/0125/c1001-26445047.html> accessed 1 September 2022.
[108] National Security Law of People's Republic of China (中华人民共和国国家安全法), An unofficial translation: chinalawtranslate.com/2015nsl/

security legislation in China, setting out the fundamental principles for conducting national security work.[109] A number of more detailed laws further established this framework, including the Counter-espionage Law (2014),[110] the Counter-terrorism Law (2015),[111] and the National Intelligence Law (2017).[112] The abovementioned laws provide legal bases for national security agencies in China to gain access to personal information for national security purposes.

5.1 Legal bases and scope

National Security Law

The Chinese National Security Law includes a section regarding the gathering of intelligence information. State organs, including state security organs, public security organs, and military organs, are authorised to '*gather intelligence information related to national security*'.[113] When carrying out intelligence information gathering efforts, the state organs must *'fully utilise contemporary scientific and technical techniques, strengthening the distinction, screening, synthesis and analytic assessment of intelligence information*'.[114]

Furthermore, the National Security Law provides state security organs and public security organs with the powers to investigate. Their investigation powers allow them to '*lawfully collect intelligence information related to national security, and perform their duties in accordance with law to investigate, detain, do pretrial work and conduct arrests as well as other duties provided by law*'.[115]

The National Security Law also specifies citizens' and organisations' obligations regarding protecting national security.[116] The obligations include *'providing evidence related to activities endangering national security*', as well as to support and assist relevant state organs with their national security works.[117] This means that technology companies may have the obligation to provide the personal information they store to support national security related works. This obligation is quite general without

[109] Yezhong Zhou (周叶中) and Yuanfu Pang (庞远福), 'On National Security Law: Models, Systems and Principles (论国家安全法:模式、体系与原则)' (2016) 07 Social Science Digest (社会科学文摘) 20.
[110] The Counter-espionage Law of the People's Republic of China (中华人民共和国反间谍法) (1 November 2014) <https://www.chinalawtranslate.com/en/anti-espionage/> accessed 21 December 2022.
[111] The Counter-terrorism Law of the People's Republic of China (中华人民共和国反恐怖主义法) (27 April 2018) <https://www.chinalawtranslate.com/en/counter-terrorism-law-2015/> accessed 21 December 2022.
[112] The National Intelligence Law of the People's Republic of China (中华人民共和国国家情报法) (27 April 2018) <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/> accessed 21 December 2022.
[113] Article 52 National Security Law.
[114] Article 53 National Security Law.
[115] Article 42 National Security Law.
[116] European Data Protection Board (n 43).
[117] Article 77 National Security Law.

mentioning an objective criterion, and might conflict with the principle of necessity under the European Essential Guarantees.

National Intelligence Law

The Chinese National Intelligence Law was adopted on 27 June 2017, and amended on 27 April 2018. The National Intelligence Law provides more detailed rules on the gathering of national intelligence.

In addition to the scope of collecting intelligence information mentioned in the National Security Law, the National Intelligence Law specifies that the means for national intelligence agencies to conduct investigation activities, includes '*entering work sites and facilities, questioning relevant institutions and individuals, collecting relevant files, materials or items*.'[118] Moreover, when necessary, national intelligence agencies may employ technical investigation measures through internal approval procedures.[119] Article 22 of the National Intelligence Law encourages national intelligence agencies to use scientific and technical techniques to increase the capacity for conducting intelligence tasks.[120]

Counter-espionage Law

The Counter-espionage Law authorises national security organs to access personal data held by individuals and organisations for counter-espionage purposes.

Moreover, the Counter-espionage Law can be applied to institutions or individuals outside the territory when they engage in espionage activities endangering national security.[121] Such institutions and individuals also include subsidiaries established in China by foreign parent companies, as well as foreigners living in China.[122] According to lower level 'Regulations on Counter-espionage Security Work', national security organs are allowed to conduct the *'inspection of electronic communication tools, equipment and other equipment and facilities'*.[123]

Counter-terrorism Law

Under the Counter-terrorism Law, national security organs and public security organs are required to gather intelligence for counter-terrorism purposes.[124] Technical measures are allowed when necessary, in accordance with the law and through internal approval procedures.[125]

---

[118] Article 16 National Intelligence Law.
[119] Article 15 National Intelligence Law.
[120] Article 22(2) National Intelligence Law.
[121] Article 6 Counter-espionage Law.
[122] Article 3 of Detailed Implementation Rules for the Counter-espionage Law (反间谍法实施细则), promulgated by the State Council on 22 November 2017. <http://www.gov.cn/zhengce/content/2017-12/06/content_5244819.htm> accessed 20 December 2022.
[123] Article 24 Regulations on Counter-espionage Security Work.
[124] Article 43 Counter-terrorism Law.
[125] Article 45 Counter-terrorism Law.

While the Counter-terrorism Law specifies that every organisation and individual has the obligation to assist and cooperate with relevant counter-terrorism activities,[126] telecommunications business operators and Internet service providers are specifically required to provide assistance to counter-terrorism work. They must *'provide a technical interface, decryption and other technical support and assistance for the prevention and investigation of terrorist activities conducted by public security authorities and national security authorities in accordance with the law'*.[127] The scope of this obligation applies to all customers. In other words, the scope is not limited to persons suspected of terrorist activities.[128] These organisations may be charged administrative fines if they do not provide such support as required.[129]

5.2 Limitations and safeguards

Under the Chinese Constitution, the state must respect and protect human rights.[130] As a general principle, this phrase has also been incorporated into the Chinese national security legislative framework and implemented in relevant laws. For instance, the National Security Law recognises the '*respect for and protection of human rights*' and '*protect the personal rights, property rights, democratic rights and other rights of citizens*' as one of the fundamental principles in national security work.[131] This principle has also been recognised in other identified laws, meaning the right to privacy, as a sort of personal rights, is also protection at least in principle against national security agencies.[132]

The general principle of protecting the rights of citizens is reflected by many articles in the Chinese national security legal framework. However, while the aforementioned laws frequently refer to the respect of physical and property rights of citizens, the right personal information is not directly mentioned. The right of privacy is only taken into account as the national intelligence agencies' confidentiality obligation.[133]

Regarding the restrictions on the access to personal information through technological investigative measures, the Counter-espionage Law mentions that national security organs can only do so *'on the basis of national provisions'*, and *'upon strict formalities for approval'*.[134]

---

[126] Article 9 Counter-terrorism Law.
[127] Article 18 Counter-terrorism Law.
[128] Cheng (程雷) (n 96).
[129] Article 84(1) Counter-terrorism Law.
[130] Article 33(4) Constitution.
[131] Article 3 National Security Law.
[132] Article 8 National Intelligence Law, Article 6 Counter-terrorism Law, Article 5 Counter-espionage Law. See, Xiaomei Liu(刘小妹), 'The National Security Law fully reflects the principle of human rights protection (《国家安全法》充分体现人权保障原则)' (2016) 08 People's Rule of Law (人民法治) 24.
[133] Article 19 National Intelligence Law, Article 48 Counter-terrorism Law, Article 17 Counter-espionage Law.
[134] Article 12 Counter-espionage Law.

More limitations are set by some lower-level rules. For instance, the Provisions on Efforts on Counter-espionage Security Precautions promulgated by the Ministry of State Security stipulate the purpose limitation principle, notification obligations and recording obligations of the national security agencies.[135]

Compared to the broad power of national security agencies to collect intelligence information, including personal information, the aforementioned limitations are still deemed vague and not specific enough.

5.3 Oversight

It has been argued that when enacting new laws at the national level in China, the law may only provide basic principles. More detailed implementing rules are to be defined in relevant lower-level regulations and policies.[136] As a result, the National Security Law does not stipulate detailed implementing rules nor enforcement and oversight mechanisms.

Similarly, the other identified laws do not provide an independent oversight mechanism regarding the powers of national security agencies either.[137] The oversight and enforcement of the law relies on the internal oversight procedure within the executive administrations.[138]

The national intelligence agencies may only access and collect relevant files, facilities or items after obtaining approval.[139] However, the approval procedure is internally established without external oversight mechanisms. Also, under urgent circumstances, no approval is needed, the staff of national intelligence agencies can access relevant information only upon presentation of their identification. Same in the Counter-espionage Law and the Counter-terrorism Law, the use of technical investigative measures needs to be based on 'strict formalities' and specific approval mechanisms.[140] However, the laws do not provide further details of such approval procedures.

Article 26 of the National Intelligence Law refers to the fact that national intelligence agencies shall supervise and oversee the staff's compliance with laws and discipline.

---

[135] Ministry of State Security, the Provisions on Efforts on Counter-espionage Security Precautions (反间谍安全防范工作规定), 26 April 2021. https://www.chinalawtranslate.com/en/counterespionage-precautions/

[136] Zongke Yang (杨宗科), 'On the Basic Legal Characteristics of the National Security Law (论《国家安全法》的基本法律属性)' (2019) 04 Journal of Comparative Law (比较法研究) 1.

[137] Lingbin Deng (邓灵斌), 'National Security and the Protection of Personal Information under the National Intelligence Act - A Review of the UK's Intelligence Surveillance System and its Lessons Learned (《国家情报法》规制下的国家安全与个人信息保护之考量——兼论英国情报监听制度及其借鉴)' (2018) 8 Journal of Information Resources Management(信息资源管理学报) 29.

[138] See Article 31 National Intelligence Law, Article 16 Counter-espionage Law.

[139] Article 16 National Intelligence Law.

[140] Article 12 Counter-espionage Law, Article 45 Counter-terrorism Law.

However, the supervision does not directly refer to the protection of citizens' rights, but more in the context of security reviews.

In summary, the national security laws in China provide broad principles for enforcing national security but lack detailed implementing rules and enforcement mechanisms. The implementation and enforcement of these laws rely on internal procedures within the executive administration, without external oversight. The absence of independent oversight also raises concerns about accountability and transparency of the oversight procedures.

5.4 Individual redress mechanisms

The Administrative Procedure Law stipulates that citizens and organisations have the right to sue an administrative organ or its staff for infringement of his or her or its lawful rights and interests.[141] As mentioned in the Criminal Procedure part, the scope is limited to material and physical infringements. The infringement of personal information cannot be regarded as a reason for such lawsuits so far.

Regarding remedies for citizens, Article 82 of the National Security Law provides citizens with the right to raise criticisms with and submit recommendations to state organs, as well as the right to file complaints and accusations, and to report unlawful activities. Such complaints are subject to internal procedures.

The National Security Law includes a section regarding the rights of citizens. Most of the protections can only cover the loss when the citizens are supporting and assisting national security work. For instance, the law protects citizens and organisations when they are '*supporting or assisting national security efforts*'.[142] Compensation can be obtained if citizens and organisations suffer a loss of asset because '*they supported or assisted national security work*'.[143]

The remedies for citizens and organisations also refer to the right to make a report or accusation about national security agencies and their staff.[144] The reasons may include '*exceeding or abusing their authority or their other unlawful conduct*'.[145] These complaints should be made directly to internal organs within the national security agencies.

According to the Counter-terrorism Law, remedies to individuals and relevant organisations cover *'compensation or indemnification'* which *'shall be made in accordance with law'*.[146]

Overall, there is no independent supervision structure in place to review data processing activities and to whom data subjects can file complaints.[147] Both the

[141] Article 2 Administrative Procedure Law.
[142] Article 80 National Security Law.
[143] Article 81 National Security Law.
[144] Article 27 National Intelligence Law, Article 26 Counter-espionage Law.
[145] Article 26 Counter-espionage Law.
[146] Article 78 Counter-terrorism Law.
[147] European Data Protection Board (n 43).

oversight mechanisms and the remedy mechanisms for individuals rely on internal procedures within the state organs. The detailed rules of oversight are largely subject to lower-level documents and instructions, which are not transparent to the public.[148]

6. Examining the Chinese legal framework in light of the European Essential Guarantees

The first European Essential Guarantee requires 'clear, precise and accessible rules'. With regard to the rules of law, the previous sections have demonstrated that there are several Chinese laws requiring and authorising state agencies to gain access to and use personal information for criminal investigation and national security purposes. The PIPL, as the first comprehensive data protection law in China, sets limitations and obligations regarding the processing of personal information for public authorities. However, our analysis found that the limitations on the powers delegated to these state agencies are sometimes quite vague and general. The PIPL might often be not clear and precise enough to be implemented against state agencies.[149]

The second Guarantee requires that 'necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated'. Our analysis found that the principle of necessity and proportionality has been referred to as a principle for personal information processing activities in the PIPL.[150] However, there are still a few specific laws authorising national security agencies to have access on a generalised basis to personal information.[151] The broad authorisation might lead to a risk of surveillance.[152]

The third Guarantee requires an independent oversight mechanism. According to the identified legal instruments, oversight of national security and criminal investigation agencies is subject to their internal oversight mechanisms. Moreover, the PIPL still fails to establish an independent authority enforcing the data protection requirements, both for private and public actors. The vulnerability of internal oversight mechanisms and the lack of an independent data protection authority continue to be problematic, at least from an EU perspective.[153] This will not only cause problems in law enforcement practice in China, but also be deemed as a barrier for the Chinese data protection framework to meet the EU's expectations regarding cross-border data transfers.

---

[148] Cheng (程雷) (n 96).
[149] Wang (王锡锌) (n 98).
[150] Article 5 and 6 PIPL.
[151] For instance, Article 77 National Security Law.
[152] Sun(孙清白) (n 46); Yanhong Liu (刘艳红), 'The theoretical basis and practical unfolding of the modernization of the trial system and trial capacity in the era of big data (大数据时代审判体系和审判能力现代化的理论基础与实践展开)' (2019) 43 Journal of Anhui University (Philosophy and Social Science Edition) (安徽大学学报哲学社会科学版) 96.
[153] Greenleaf (n 67).

Lastly, the fourth Guarantee requires effective remedies for individuals. In China, individuals have right to file a complaint, make a report or an accusation in the event of unlawful processing of personal data, or claim compensation for data privacy breaches. As such, these rights rely upon the internal oversight department of each state organ to provide a remedy, rather than the 'legal action before an independent court' as required by the European standards.[154]The legislation analysed by this paper is summarised in the table below.

Laws		Clear, precise and accessible rules	Necessity and proportionality	Oversight	Redress
General legal framework	Personal Information Protection Law	Public authorities fall within the scope of the PIPL. Specific limitations for public authorities: legality and necessity, notification, data localisation.	The principle of necessity and proportionality has been referred to as a principle for personal information processing activities in the PIPL	Internal oversight	Complaints to internal oversight departments; compensation for data privacy breaches; class-action suits.
Criminal investigation purposes	Criminal Procedure Law	People's courts, people's procuratorates and public security organs are required to gather and collect evidence (including electronic data as a form of evidence). The means of gathering evidence include search and seizure and technical investigation measures.	Warrant based on internal procedures.	Internal oversight	Infringement of personal information is not yet a basis to sue criminal investigation agencies.
National security purposes	National Security Law	Authorising national security organs, public security organs and military organs to gather intelligence information related to national security, by means of fully utilising contemporary scientific and technical techniques. Citizens and organisations are obliged to support and assist.	Respect of citizens' lawful rights and interests.	Internal oversight	Raise criticism and recommendations, file complaints, accusations and report unlawful activities.
	National Intelligence Law	State security organs, public security organs and military intelligence institutions are authorised to gather national intelligence. Citizens and organisations are obliged to support and assist. Technical measures may be employed.	Strictly in accordance with the law, must not exceed or abuse their authority and must not violate the lawful rights and interests of citizens and organizations.	Internal oversight	Make a report or accusation.
	Counter-espionage Law	State organs are empowered to check electronic communication tools, equipment and other facilities. Citizens and organisations are obliged to support and assist. Technical measures may be employed.	Having internal approval before employing technological investigative measures.	Internal oversight	Raise criticism and recommendations, file complaints, accusations and report unlawful activities.
	Counter-terrorism Law	Citizens and organisations are obliged to support and assist. Telecommunication business operators and Internet service providers are required to provide specific assistance to counter-terrorism work. Technical measures may be employed.	Having internal approval before employing technological investigative measures.	Internal oversight	Compensation or indemnification.

[154] European Data Protection Board (n 5) para 47.

7. Conclusion

This paper has analysed the Chinese legal framework regarding public authorities' access and use of personal information, and has analysed these legal instruments from the perspective of the European Essential Guarantees. Based on the conducted analysis, it can be concluded that the current Chinese legislative framework regarding government access and use of personal data sometimes remains general and insufficient.[155] These gaps will continue to be a barrier to China's framework being deemed as 'essentially equivalent' to the EU's data protection level in the near future. This may cause legal uncertainty for both the European and the Chinese businesses conducting cross-border data transfers from the EU to China.[156]

From a Chinese perspective, the recent developments regarding the Chinese data protection framework are positive. The PIPL is the first comprehensive data protection law and the first law in China regulating public authorities' processing of personal information. For Chinese policymakers, there is an urgent need to promulgate a specific administrative law governing the processing of personal information for law enforcement and national security purposes by public authorities. Meanwhile, more detailed rules to effectively implement the data protection principles against public authorities are also needed. In this context, the EU's approach may also provide a path forward: government access and use of personal information needs to be regulated with clearer limitations to the investigation powers, necessity and proportionality tests, effective oversight mechanisms and effective individual remedies.

[155] Geller (n 69).
[156] Nottingham (n 4).