DOI 10.5817/MUJLT2024-2-1

PEOPLE'S REPUBLIC OF CHINA AND THE ADEQUACY – WHY CHINESE DATA PROTECTION LAW IS NOT ADEQUATE WITHIN THE MEANING OF THE GDPR*

by

WOJCIECH PANEK †

Chinese data protection seems to be problematic. On the one hand, it does exist, at least formally, especially after the reform initiated by the adoption of the Cybersecurity Law and finished by the Personal Information Protection Law entering into force. However, the mere adoption of personal data protection regulations does not guarantee that they provide personal data protection at an appropriate level. For EU law, the adequacy standard is the reference point for verifying personal data protection in a third country. Therefore, it is necessary to meet specific criteria summarising the term of essential equivalence, as introduced by the Court of Justice of the European Union. This article discusses the three most critical problems that result from comparing the provisions of the Chinese Cybersecurity Law, the Civil Code, the Data Security Law and the Personal Information Protection Law with the EU's adequacy standard. The article consists of the introduction, four parts and closing remarks. The first part explains the methodology of research on Chinese data protection law and criteria applied to its examination. The second, third and fourth parts discuss the complicated relationships between the laws related to the protection of personal data, the status of state authorities as data controllers and multi-stakeholder supervision over personal data protection.

* Part of the research project "Transfer of Personal Data between the European Union and the People's Republic of China. Legal aspects", financed from the Preludium-19 grant from the National Science Centre's (Narodowe Centrum Nauki) (contract number UMO 2020/37/N/HS5/01799).

† At the time of writing this paper, the Author was a PhD student at Doctoral School at the University of Silesia in Katowice. ORCID: 0000-0003-3264-986x. For correspondence: wojciech.panek@us.edu.pl

KEY WORDS
GDPR, Adequacy, Personal Data Transfers, China, Data Protection in China.

1. INTRODUCTION
Is there any data protection in the People's Republic of China[1]? The answer to that question is not as straightforward as one might expect. Through several recent reforms, the Chinese legal system of data protection has undergone far-reaching changes. It all started in October 2017 and – probably – finished in October 2021. The first date refers to the adoption of the Cybersecurity Law[2], a cybersecurity-oriented regulation. The fact that it included data protection provisions led to the doctrine declaring it a milestone in developing contemporary data protection law in China.[3] The second date is when the Personal Information Protection Law[4] came into force. In the meantime, some other data-protection-related regulations were enacted[5]. Hence, the Chinese data protection law currently comprises the Cybersecurity Law and the Personal Information Protection Law[6], supplemented by the Chinese Civil Code[7] and the Data Security Law[8].

The mere existence of data protection law does not necessarily amount to actual data protection. The latter depends on the quality of that law.

---

1 Hereinafter referred to as China

2 Zhonghua Renmin Gonghegup Wanglup Anquan Fa (中华人民共和国网络安全法) [Cybersecurity Law of the People's Republic of China] (issued by the Standing Committee of the National People's Congress on 11 July 2016, came into force on 1 June 2017, bilingual version accessed via PKU Law database).

3 Pernot-Leplay, E. (2020) China's Approach on Data Privacy Law: A Third Way between the U.S. and the EU? *Penn State Journal of Law and International Affairs*, 8(1), p. 71.

4 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] (issued by the Standing Committee of the National People's Congress on 20 August 2021, came into force on 1 November 2021, bilingual version accessed via PKU Law database).

5 These are: Zhonghua Renmin Gongheguo Minfa Dian (中华人民共和国民法典) [Civil Code of of the People's Republic of China] (issued by the National People's Congress on 28 May 2020, came into force on 1 January 2021, bilingual version accessed via PKU Law database) and Zhonghua Renmin Gongheguo shuju Anquan Fa (中华人民共和国数据安全法) [Data Security Law of the People's Republic of China] (issued by the Standing Committee of the National People's Congress on 10 June 2021, came into force on 1 September 2021, bilingual version accessed via PKU Law database).

6 Guangping, W. (2021) Challenges and Responses to the Protection of Workers' Personal Information in the Context of Human-Computer Interaction. *China Legal Science*, 9(139), pp. 144-145.

7 Gao, R. Y. (2020) Personal Information Protection under Chinese Civil Code: A Newly Established Private Right in the Digital Era. *Tsinghua China Law Review*, 13 (1), p. 183.

8 Cai, P., Chen, L. (2022) Demystifying data law in China: a unified regime of tomorrow. *International Data Privacy Law*, 12(2), p. 78; Chen, J. Sun, J. (2021) Understanding the Chinese Data Security Law. *International Cybersecurity Law Review*, 2, p. 218.

The uncertain effectiveness of Chinese data protection legislation[9] stems from purpose of the reform clearly set out by the Chinese authorities. The overarching purpose was to diminish the influence of lacking data protection laws on economic relations with Western entities, yet with Chinese specificity.[10] Consequently, the protection of the data subject, well-known from the GDPR and EU legislation, was not the central theme of the reform and abovementioned regulations.[11] Instead the focus was primarily on business needs, mainly the need for undisturbed technological development, combined with political factors.[12]

With this background in mind, it would not be shocking to say that the reform brought nothing to data subjects. However, the overall impression of the Chinese data protection law[13] suggests something different as the legislation encompasses data protection principles, data subject's rights, sanctions for data controllers and establishes some data authorities.

EU data protection law takes a strict attitude[14] towards personal data transfers outside the EU[15]. Though, any remarks concerning the content

[9] Cai, P., Chen, L. Demystifying data law in China: a unified regime of tomorrow. *International Data Privacy Law*, 12(2), p. 92; Zheng, G. (2021) Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S. and China. *Computer Law & Security Review*, 43, p. 6.

[10] See: Creemers, R. (2021) China's Emerging Data Protection Framework. *Journal of Cybersecurity*, 8(1), p. 14.

[11] Creemers, R. (2021) China's Emerging Data Protection Framework. *Journal of Cybersecurity*, 8(1), p. 14; Zhao, B., Feng, Y. (2021) Mapping the development of China's data protection law: Major actors, core values, and shifting power relations. *Computer Law & Security Review*, 40, p. 11.

[12] Feng, Y. (2019) The future of China's personal data protection law: challenges and prospects. *Asia Pacific Law Review*, 27 (1), p. 64.; Zhao, B. (2021) Connected Cars in China: Technology, Data Protection and Regulatory Responses. In: Alexander Roßnagel, Gerrit Hornung (eds.). *Grundrechtsschutz im Smart Car. DuD-Fachbeiträge*. Wiesbaden: Springer Vieweg, p. 21.; Liu, J. (2020) China's data localization. *Chinese Journal of Communication*, 13 (1), p. 91.; Trakman, L., Walters, R., Zeller, B. (2020) Digital consent and data protection law – Europe and Asia-Pacific experience. *Information & Communications Technology Law*, 29 (2), p. 233.; Creemers, R. (2021) China's Emerging Data Protection Framework. *Journal of Cybersecurity*, 8(1), p. 14; Zhao, B., Feng, Y. Mapping the development of China's data protection law: Major actors, core values, and shifting power relations. *Computer Law & Security Review*, 40, pp. 6; 12.; You, C. (2022) Half a loaf is better than none: The new data protection regime for China's platform economy. *Computer Law & Security Review*, 45, p. 16.

[13] The Cybersecurity Law, the Personal Information Protection Law, supplemented by the provisions of the Chinese Civil Code and the Data Security Law, hereinafter referred to as the Chinese data protection law.

[14] Schantz, P. (2023) Article 44 GDPR. In: Spiecker gen. Döhmann et al. (eds.). *General Data Protection Regulation: Article-by-Article Commentary*. Nomos, p. 777; Kuner, C. (2020) Article 44 GDPR. In: Christopher Kuner et al. (eds.). *The EU General Data Protection Regulation (GDPR). A commentary*. Oxford University Press, p. 757.

[15] By virtue of Article 44, the GDPR only allows personal data to be transferred to a third country which has demonstrated it provides for an acceptable level of data protection. If there is an adequate level of data protection, then under Article 45 GDPR, the European Commission

of a third country's data protection law automatically bring about the concept of adequacy, as set out in the GDPR[16]. Reflecting the EU's attitude towards personal data transfers outside the EU, the adequacy standard sets a benchmark for assessments of similarities or differences between EU and third countries' laws.[17] In a nutshell, the adequacy standard requires the third-country data protection law to offer a level of data protection equivalent to that arising from EU law, particularly from the GDPR[18]. As further explained by the Court of Justice of the European Union in Schrems I and Schrems II cases, the third-country's legal system must be essentially equivalent, which means there is no need for the third-country legal system to be the same as that of the EU. Nevertheless, a third country must provide data subjects with fundamental rights that are enforceable and must organise the data processing activities in line with the data protection principles under the supervision of an independent data protection authority.[19]

In this paper, I discuss the level of data protection stemming from the Chinese data protection law. The paper presents partial result of my research project on Chinese data protection law.[20] While conducting research, I answered the following research question: does Chinese data protection law meets the criteria derived from the adequacy concept? The analysis proved that Chinese data protection law[21] does not meet the adequacy criteria, and as a result, falls short compared to the GDPR and EU law. Due to the limited

is entitled to issue an adequacy decision. In that case personal data can be transferred to a third country without limitations. If not, there should be no transfer of personal date to that country, unless the data controller implements appropriate safeguards of Article 46 GDPR or relies on one of derogation of Article 49 GDPR.

16 Schantz, P. (2023) Article 44 GDPR. In: Spiecker gen. Döhmann et al. (eds.). *General Data Protection Regulation: Article-by-Article Commentary*. Nomos, p. 777-778; Kuner, C. (2020) Article 45 GDPR. In: Christopher Kuner et al. (eds.). *The EU General Data Protection Regulation (GDPR). A commentary*. Oxford University Press, p. 775.

17 Thoughts on the expected level of data protection in a third country are presented, among others, by Schwartz P.M. (1995) European Data Protection Law and Restrictions on International Data Flows. *Iowa Law Review,* 80(3), p. 471, 473, 487; Blume P. (2015) EU Adequacy Decisions: The Proposed New Possibilities. *International Data Privacy Law*, 5(1), p. 34; also: Gulczyńska Z. (2021) A certain standard of protection for international transfers of personal data under the GDPR. *International Data Privacy Law*, 11(4), p.34.

18 Schantz, P. (2023) Article 45 GDPR. In: Spiecker gen. Döhmann et al. (eds.). *General Data Protection Regulation: Article-by-Article Commentary*. Nomos, p. 789-790.

19 Judgement of 6 October 2015 *Maximillian Schrems v Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650, hereinafter referred to as Schrems I; Judgement of 16 July 2020 *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*, C-311/18, ECLI:EU:C:2020:559, hereinafter referred to as Schrems II.

20 Devoted to the problem of data transfers between China and European Union

21 The Cybersecurity Law, the Personal Information Protection Law, supplemented by the provisions of the Chinese Civil Code and the Data Security Law, hereinafter referred to as the Chinese data protection law.

volume of this paper, which makes it impossible to present an in-depth description of the results, I decided to focus on three main disparities of Chinese data protection law from the EU law model namely:

- the complicated structure of personal data protection law landscape,
- the doubtful application of data controller definition to state bodies,
- the lack of a dedicated data protection authority in China.

Nevertheless, there are also other problems, in particular the interpretative concerns related to the rights of data subjects granted by the Cybersecurity Law, the Civil Code, the Data Security Law and the Personal Information Protection Law, or the data protection principles they mention[22]. In addition, the overall level of personal data protection in China is also affected by the widely cited cases of surveillance of individuals by state authorities and the associated access to personal data by state authorities[23].

The paper consists of four parts. In the first part, I briefly describe the methodology of the assessment of the Chinese data protection law. The second, third and fourth parts discuss in detail the drawbacks of the Chinese data protection law, to end with concluding remarks.

2. ASSESSING A THIRD COUNTRY'S LEGAL SYSTEM – THE INFLUENCE OF THE GDPR'S ADEQUACY STANDARD ON THE ASSESSMENT OF THE CHINESE DATA PROTECTION LAW

I analysed the Chinese data protection law with the following criteria:

- Criterion of core data principles,
- Criterion of a data subject's enforceable rights,
- Criterion of a competent, independent supervisory authority,
- Criterion of a data subject's remedies in the event of a data breach,

[22] See inter alia: Pernot-Leplay, E. (2020) China's Approach on Data Privacy Law: A Third Way between the U.S. and the EU? *Penn State Journal of Law and International Affairs*, 8(1), p. 53-54, 77-78; Wang Han, S. Munir, A.B. (2018) Information Security Technology – Personal Information Security Specification: China's Version of the GDPR? *European Data Protection Law Review*, (4) 4, p. 535.

[23] See inter alia: Shao, Y. (2021) Personal Information Protection: China's Path Choice. *US-China Law Review*, 18(5), p. 236; Pernot-Leplay, E. (2020) China's Approach on Data Privacy Law: A Third Way between the U.S. and the EU? *Penn State Journal of Law and International Affairs*, 8(1), p. 107;

- Criterion of access to data by public authorities in the third country.

The choice of criteria included in the assessment was based on comprehensive analysis of adequacy concept.[24] Although the adequacy assessment procedure is still not transparent enough[25], the doctrine explained that content of the adequacy assessment arises from four elements[26]:

1) Article 45 of GDPR and with its assessment criteria.

2) The European Data Protection Board guidelines[27].

It is worth emphasising that the guidelines issued by the European Data Protection Board and its predecessor[28] are the only official comment on the adequacy assessment. Consequently, the assessment debate often amounts to mostly a discussion of these guidelines

3) The jurisprudence of Court of Justice of the European Union[29].

Since 2015, the Court of Justice of the European Union has played a significant role in the third-country assessment. For the purpose of this article, it is enough to say that the Schrems I judgement explains the required level of data protection in the third country by introducing the essential equivalence concept. Moreover, it creates an additional criterion for assessing

[24] More detailed description of this part of my research I present in the following paper: Panek, W (2024) The European Commission's adequacy decisions' content as a guide for applying the adequacy assessment criteria. The paper awaits publication in the Privacy Symposium Proceedings 2024 (Springer).

[25] Kuner, C. (2009) Developing an Adequate Legal Framework for International Data Transfers. In: Serge Gutwirth, et al. (eds.). *Reinventing Data Protection?* Springer Science+Business Media B.V., p. 268.; Makulilo, A. B. (2013) Data Protection Regimes in Africa: too far from the European 'adequacy' standard? *International Data Privacy Law*., 3(1); Kuner, C. (2017) Reality and Illusion in EU Data Transfer Regulation Post Schrems. *German Law Journal*, 18 (4), pp. 900–901. Also, see: Czerniawski, M. (2021) Rola Komitetu Art. 93 RODO w procedurze oceny adekwatności państw trzecich. *Gdańskie Studia Prawnicze*, 25(4), pp. 106-126.

[26] See: Blume, P. (2015) EU Adequacy Decisions: The Proposed New Possibilities. *International Data Privacy Law*, 5(1); Gulczyńska, Z. (2021) A certain standard of protection for international transfers of personal data under the GDPR. *International Data Privacy Law*, 11(4); Kuner, C. (2009) Developing an Adequate Legal Framework for International Data Transfers. In: Serge Gutwirth, et al. (eds.). *Reinventing Data Protection?* Springer Science+Business Media B.V., p. 268.; Makulilo, A. B. (2013) Data Protection Regimes in Africa: too far from the European 'adequacy' standard? *International Data Privacy Law*., 3(1); Kuner, C. (2017) Reality and Illusion in EU Data Transfer Regulation Post Schrems. *German Law Journal*, 18 (4), pp. 900–901.

[27] European Data Protection Board (2017) Adequacy Referential (WP 254 Rev.01, 28 November 2017) hereinafter referred to as a WP254.

[28] Article 29 Working Party (1998) Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive (WP12, 24 July 1998) hereinafter referred to as WP12.

[29] Schrems I and Schrems II.

adequacy, namely the access to personal data by third countries' authorities. The Schrems II judgment sustains and confirms both concepts.[30] At the same time, it expands on using the Charter of Fundamental Rights as the assessment criterion.

4) The adequacy decisions issued to date[31].

The analysis of four elements mentioned above allowed me to reconstruct the list of criteria that are crucial when assessing a third country's legal system. When it comes to the content of each criterion, the doctrine and the European Commission is highly influenced by its understanding propose by the EDPB[32]. Consequently, the meaning of core data principles' criteria, data subject's enforceable rights, competent, independent supervisory authority and data subject's remedies in the event of a data breach is derived from EDPB guidelines WP254. For the criterion of data access by public authorities in a third country, the EDPB created
a separate document which in detail explains the meaning of that criterion.[33]

Before commencing the discussion on the subject matter, I would like to draw the reader's attention to another detail. The abovementioned criteria, used for assessing Chinese data protection law, do not address the criterion of human rights protection. Surprising as it might be, this attitude reflects the vague nature of adopting human rights criterion, which is part and parcel of all the adequacy decisions issued so far.[34] Under Article 45 GDPR, the European Commission is obliged to verify human rights protection and respect for rules of law in the examined third country.[35] However, in practice, none of the adequacy decisions referred to these criteria in their content.[36] The same might be said about the European Data Protection Board

[30] However, Bradford et. al. claim that Schrems II judgement has made the adequacy much stricter – see Bradford L., Aboy M., Liddell K. (2021) Standard Contractual Clauses for Cross-Border Transfers of Health Data after Schrems II. *Journal of Law and the Biosciences*, 8 (1), p. 11 - 17

[31] Past decisions are relevant because they show which criteria apply and to what extent.

[32] Stemming from WP254.

[33] European Data Protection Board (2020) Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

[34] Another example is the criterion of international commitments. Within GDPR-based adequacy decisions, only the UK's decision contains the European Commission's affirmation of ratification of the Council of Europe Convention No 108 and mentions the Convention for the Protection of Human Rights and Fundamental Freedoms.

[35] Kuner, C. (2021) The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards. *National Law Review of India*, 33(1), p. 80; Wittershagen, L. (2023) Transfer of Personal Data to Third Countries under the European Data Protection Law. In: Leonie Wittershagen (ed.) *The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit*. De Gruyter, p. 59,

[36] The doctrine has noticed the inconsistent approach of the European Commission when assessing third countries in this respect – see Wolf C. (2013) Delusions of Adequacy -

guidelines, where no reference was made to the criterion of human rights protection.

This attitude might be explained by political background involvement. C. Kuner believes that the adequacy assessment is also related to background political pressure, not only the protection of personal data as such.[37] Bradford explains the political background by referring to trade or cultural relationships, or strategic objectives that stand behind the need for continuous data flow.[38] Therefore, the political background sometimes amounts to the criterion of supporting business relations between the European Union and the examined third country. First and foremost, this is the case in the EU – USA transfers. Graham Greenleaf finds justification for an imperfect adequacy standard arising from the Safe Harbour decision in American economic power and its influence on Europe.[39] Other third countries are in a different position because, as Greenleaf says, 'other countries do not have the economic muscle of the US.'[40] Economic relations are often mentioned during discussions about the adequacy of Israel or Argentina. Some authors say that these countries are adequate as they can be found among the close trading partners of the European Union.[41] For that reason, despite identified shortcomings, they were granted adequacy

Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers. *Washington University Journal of Law & Policy*, 43, p. 240-241.

37 Kuner, C. (2009) Developing an Adequate Legal Framework for International Data Transfers. In: Serge Gutwirth, et al. (eds.). *Reinventing Data Protection?* Springer Science+Business Media B.V., p 267. The problem of considering the political background is also mentioned by: Makulilo, A.B, (2013) Data Protection Regimes…, p. 49; Blume, P. (2000) Transborder Data Flow: Is There a Solution in Sight. *International Journal of Law and Information Technology*, 8(1), p. 69

38 Bradford, L., Aboy, M., Liddell, K. (2021) Standard Contractual Clauses for Cross-Border Transfers of Health Data after Schrems II. *Journal of Law and the Biosciences*, 8 (1), p. 14.

39 Greenleaf, G. (2000) Safe Harbor's low benchmark for 'adequacy': EU sells out privacy for US$. *Privacy Law and Policy Reporter*, 7(3), p. 45.

40 Ibid.

41 Roth P. (2017) Adequate level of data protection' in third countries post-Schrems and under the General Data Protection Regulation. *Journal of Law, Information and Science,* 25(1), p. 49; Blackmore N. (2019) Feeling inadequate? Why adequacy decisions are rare (and may get rarer) in Asia-Pacific. *Kennedys* 26 March, available from: `https://kennedyslaw.com/thought-leadership/article/feeling-inadequate-why-adequacy-decisions-are-rare-and-may-get-rarer-in-asia-pacific/` [accessed 17 October 2022].

decisions[42], while for other countries same shortcomings somehow made it impossible to find those third countries adequate.[43]

Interestingly, the political background discussed above finds support of European Parliament. In its resolutions referring to data transfers to the USA, the European Parliament emphasised the importance of economic relations and their influence on the subject matter.[44]
A similar view can be found in a paper related to data transfers between the European Union and China. Here, economic relations were used as an argument for a less strict, more practical, and realistic attitude to assessing the Chinese legal system.[45]

In my opinion, business relations should have no sway in terms of turning a blind eye to human rights infringements. I agree with Drechsler and Kamara that violations of human rights and a disrespect for the rule of law should disqualify any country from being found adequate within meaning of the GDPR.[46] Therefore, it seems evident that human rights infringement in China are still a major obstacle to the adequacy decision being granted. In next part of this paper, I elaborate on the identified shortcomings of Chinese data protection law. Their existence has a significant influence on the standard of data protection in China. Nevertheless, even the best data

[42] In case of Israel it is said that the assurances of its representatives were considered sufficient guarantees of adequate level of data protection – Tene, O.(2022) Data transfer theatre: The US and Israel take the stage. *Privacy Perspectives*, 4 October, available from: https://iapp.org/news/a/data-transfer-theater-the-us-and-israel-take-the-stage/ [accessed 17 October 2022]; similar view expressed by Yablonko, Y. (2020) Israel's outdated privacy laws jeopardize relations with EU. *Globes*, 23 July, available from: https://en.globes.co.il/en/article-israels-outdated-privacy-laws-jeopardize-relations-with-eu-1001337077 [accessed 17 October 2022].

[43] As in the case of Burkina Faso – see Wolf C. (2013) Delusions of Adequacy - Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers. *Washington University Journal of Law & Policy*, 43, p. 240-241.

[44] Resolution of European Parliament (2016) Transatlantic data flows. Official Journal (C 76/82) 26 May. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A52016IP0233; the European Parliament refers to one of the communications of the European Commission - European Commission Communication (2013) Rebuilding Trust in EU-US Data Flows. COM 846 final, 23 November. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013DC0846.

[45] de Hert, P. Papakonstantinou, V. (2015) The data protection regime in China. In-depth analysis. European Union, p. 8. Available from: https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA\%282015\%29536472_EN.pdf.

[46] Drechsler, L., Kamara, I. (2022) Essential equivalence as a benchmark for international data transfers after Schrems II. In: Eleni Kosta, Ronald Leenes, Irene Kamara (eds.). *Research Handbook on EU Data Protection Law*. Edward Elgar Publishing, p. 235.

protection legislation means nothing in a legal system where human rights are violated[47].

3. WHICH LAW APPLIES? THE COMPLICATED STRUCTURE OF THE CHINESE DATA PROTECTION LAW SYSTEM

Chinese data protection legislation is composed of many different laws and regulations. That was the most discussed feature of Chinese law before the enactment of the Cybersecurity Law, where data-protection-related provisions were scattered among various laws, such as criminal law or consumer protection law, with no regulation of the general scope and application[48]. The reform was supposed to change this, as a specific complete data protection law was highly desired.

Initially, it was the Cybersecurity Law to be described as an example of general and comprehensive data protection law.[49] Nevertheless, some of the authors explained that personal data protection within the Cybersecurity Law was only an additional element and the legislation refers primary to cybersecurity in China.[50] Also, the Cybersecurity Law does not cover the processing of analogue personal data.[51] Hence, when the Personal Information Protection Law came into force, the doctrine changed its views

[47] It also must be noted that before the Cybersecurity Law came into force, the main obstacle to recognising Chinese legal system as adequate within the meaning of EU data protection law was the numerous problems with the state's approach to protecting human rights. However, the adoption and subsequent implementation of the Cybersecurity Law, Civil Code, Data Security Law, and Personal Information Protection Law caused the discussion on the adequacy of Chinese law within the meaning of the GDPR to no longer be limited to broadly understood issues of protecting fundamental rights. What matters now is also the quality of the provisions introduced by these laws, as these provisions should implement effective data-protection-oriented solutions that will meet the adequacy criteria referred to above.

[48] Gao, R. Y. (2020) Personal Information Protection under Chinese Civil Code: A Newly Established Private Right in the Digital Era. *Tsinghua China Law Review*, 13(1), p. 183; Duoye, X. (2020) The Civil Code and the Private Law Protection of Personal Information. *Tsinghua China Law Review*, 13(1), p. 188.

[49] Qi, A., Shao, G., Zheng, W. (2018) Assessing China's Cybersecurity Law. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 34(6), p. 7; Yuexin, Z. (2019) Cyber Protection of Personal Information in a Multi-Layered System. *Tsinghua China Law Review*, 12(1), p. 167,169.; Shao, Y. (2021) Personal Information Protection: China's Path Choice. *US-China Law Review*, 18 (5), p. 239; Tiwari, A. (2022) The Comparison between Indian Personnel and PRC New Civil Code, Cyber Laws, and Privacy. *Jus Corpus Law Journal*, 3, p. 367, 368, 377.

[50] Vecellio Segate, R. (2020) Litigating Trade Secrets in China: An Imminent Pivot to Cybersecurity? *Journal of Intellectual Property Law & Practice*, 15(8), p. 649, 650

[51] Wang Han S., Munir A.B. (2018) Information Security Technology – Personal Information Security Specification: China's Version of the GDPR? *European Data Protection Law Review*, (4) 4, p. 53.

and started to see the latter as general and comprehensive data protection law.[52]

At the same time, the role of the Data Security Law started to clarify.[53] According to Article 3 Data Security Law, the data protected by the law amounts to any information recorded, notwithstanding its form[54]. Although it covers a much broader scope of data[55] for some authors, it became evident that the Personal Information Protection Law refers to the processing of personal data, while the Data Security Law deals with the rest.[56] Thus, the link between the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law became clearer.[57]

However, one should also remember those provisions of the Chinese Civil Code that touch upon the issue of data protection. These include Articles 111 and 1034 - 1039. According to Zhou, the Civil Code, the Personal Information Protection Law and the Data Security Law present a comprehensive view of personal data protection in China.[58] This is because it is through the provisions of the Civil Code the principles of personal data protection, discussed only partially in the Cybersecurity Law, along with specific definitions given there, became universally applicable law.[59]

---

[52] Yan Wang, C. (2022) Governing Data Markets in China: From Competition Litigation and Government Regulation to Legislative Ordering. *George Mason International Law Journal*. 13(1), p. 39.

[53] Dorwart, H. (2021) Platform regulation from the bottom up: Judicial redress in the United States and China. *Policy & Internet*, 14(2), p. 377.

[54] That is because motives of cyberspace sovereignty and the protection of national security stand behind the Data Security Law.

[55] Personal data are not excluded from the definition of data.

[56] Cai, P., Chen, L. (2022) Demystifying data law in China: a unified regime of tomorrow. *International Data Privacy Law*, 12(2), p. 78. Interestingly, for relations between the Data Security Law and the Cybersecurity Law, it was the national security protection to be the explanation - Guangping, W. (2021) Challenges and Responses to the Protection of Workers' Personal Information in the Context of Human-Computer Interaction. *China Legal Science*, 9(139), p. 146; Cai, P., Chen, L. (2022) Demystifying data law in China: a unified regime of tomorrow. *International Data Privacy Law*, 12(2), p. 90.

[57] Chaskes, W. (2022) The Three Laws: The Chinese Communist Party Throws down the Data Regulation Gauntlet. *Washington and Lee Law Review*, 79(3), p. 1173.

[58] Zhou, Q. (2023) Whose data is it anyway? An empirical analysis of online contracting for personal information in China. *Asia Pacific Law Review*, 31 (1), p. 74.

[59] Berti, R. (2020) Data Protection Law: A Comparison of the Latest Legal Developments in China and European Union. *European Journal of Privacy Law & Technologies*, 1, p. 51..; Gao, R. Y. (2020) Personal Information Protection under Chinese Civil Code: A Newly Established Private Right in the Digital Era. *Tsinghua China Law Review*, 13(1), p. 174.; Duoye, X. (2020) The Civil Code and the Private Law Protection of Personal Information. *Tsinghua China Law Review*, 13(1), p. 188; Guangping W (2021) Challenges and Responses to the Protection of Workers' Personal Information in the Context of Human-Computer Interaction. *China Legal Science*, 9(139),, pp. 141–142.; Shao, Y. (2021) Personal Information Protection: China's Path Choice. *US-China Law Review*, 18 (5), p. 239.

The concise description of the various data protection laws in China, presented above, suggests that the reform's principal effect was to further complicate an already perplexing legal system.[60] Although the legislator established the applicability of the Cybersecurity Law, the Civil Code, the Data Security Law and the Personal Information Protection Law in addition to the existing provisions, it is in vain to find provisions in any of these laws clarifying the scope of their application. What is lacking is the lawmaker's clearly expressed intention regarding the scope of application of Chinese data protection laws[61]. As Greenleaf points out, the Personal Information Protection Law – the most advanced personal data protection law – does not by itself repeal the previously binding provisions related to the same issues, which means, among other things, the duplication of obligations or slightly different wording of the same obligations.[62] For other authors the Cybersecurity Law the Data Security Law and the Personal Information Protection Law have similar background[63]. Because of that, all three laws should apply to every personal data processing activity within Chinese jurisdiction, whilst only factual analysis of the case might lead to exclusion of one of them[64]. Such an interpretation means that under the threat of sanctions provided by the Cybersecurity Law, Data Security Law, and Personal Information Protection Law it is data subject or controller to decide which law they should abide, by accurately construe their current situation[65]. In such a situation, it is common to have doubts about the leading role of one of these laws, the existing catalogue of data protection principles that absolutely must be implemented and complied with, or the interplay between the different principles under the various laws.

---

[60] The expected streamlining and unification of legal data protection in China has yet to arrive.

[61] General and ambiguous provisions of data protection laws are not helpful too.

[62] Greenleaf, G. (2020) China issues a comprehensive draft data privacy law. *Privacy Laws & Business International Report*, 1, p. 12.

[63] Belli L., Doneda D. (2023) Data protection in the BRICS countries: legal interoperability through innovative practices and convergence. *International Data Privacy Law*, 13 (1), p. 82, 86, 87

[64] Cai P., Chen L. (2022) Demystifying data law in China: a unified regime of tomorrow. *International Data Privacy Law*, 12(2), p. 78-79; also: Greenleaf G. (2020) China issues a comprehensive draft data privacy law. *Privacy Laws & Business International Report*, 1, p. 12; Dorwart H. (2021) Platform Regulation from the Bottom up: Judicial Redress in the United States and China. *Policy & Internet*, 14(2), p. 379; Chaskes W. (2022) The Three Laws: The Chinese Communist Party Throws down the Data Regulation Gauntlet. *Washington and Lee Law Review*, 79(3), p. 1173; Xing H. (2023) Government Data Sharing and Personal Information Protection. *Administrative Law Research*, 2, p. 72; Zhou Q. (2023) Whose data is it anyway? An empirical analysis of online contracting for personal information in China. *Asia Pacific Law Review*, 31 (1), p. 74.

[65] While the interpretation of Chinese law will pose less of a challenge for local market players, the position of foreign players is far worse.

In conclusion, the coexistence of the Cybersecurity Law, Civil Code, Data Security Law, and Personal Information Protection Law means that the Chinese personal data protection is too complicated for the average recipient to understand. Theoretically, this is not such a severe defect as one might expect but in practice the complexity of China's personal data protection regulations results in a lack of transparency regarding the protection this system should provide. In other words, the individual, i.e. the entity whose rights and freedoms are to be protected, is not entirely sure where the protection they can invoke comes from. As a result, especially on daily basis, an individual may face a refusal to comply with a request under Law X because, according to the data controller, it is actually Law Y that covers this case, and Law Y does not include the right that the individual is invoking. Therefore, it is dubious to discuss the effective protection of personal data expected by the EU adequacy standard.

4. THE SCOPE OF CONTROLLER DEFINITION - IS A STATE BODY A DATA CONTROLLER?

From the perspective of the GDPR, state authorities that determine purposes and means of data processing are data controllers. This interpretation is not in doubt. However, based on China's data protection laws, no such statement is apparent.

The Personal Information Protection Law is the only law that contains a definition of data controller. As in the GDPR, what makes an entity a data controller within the Chinese definition is determining the means and purposes of personal data processing. The doctrine has no clear position regarding the possibility of considering a state authority as a data controller. Some authors automatically limit themselves to purely theoretical considerations when discussing the concept of the state authority as a data controller.[66] The justification for this approach is supposed to be a pragmatic approach to the surrounding reality[67] – a reality in which it is highly questionable to consider a state authority as a data controller. The reason why the state authorities would not fall within the definition of controller are consequences. As Bethany Allen-Ebrahimian once said, "Privacy, in the

[66] Ibid.; Dorwart, H. (2021) Platform regulation from…, p. 379; Chaskes. W. (2022) The Three Laws: The Chinese Communist Party Throws down the Data Regulation Gauntlet. *Washington and Lee Law Review*, 79(3), p. 1173.; Xing, H. (2023) Government data sharing and personal information protection. *Administrative Law* Research, 2.; Zhou, Q. (2023) Whose data is it anyway? An empirical analysis of online contracting for personal information in China. *Asia Pacific Law Review*, 31 (1), p. 74.

[67] Duoye, X. (2020) The Civil Code and the Private Law Protection of Personal Information. *Tsinghua China Law Review*, 13(1), p. 191.; Cai P., Chen L. (2022) Demystifying data law in China: a unified regime of tomorrow. *International Data Privacy Law*, 12(2), p. 92.

Chinese government's eyes, means privacy from other non-state actors — not privacy from the government."[68] A positive answer and application would imply a complete change in the approach to processing personal data by state bodies, which then should act in accordance with the law and thus comply with the obligations addressed to controllers. This is not what Chinese authorities need. More broadly, their status is necessary and convenient for the state authorities to still be able to carry out their surveillance activities.[69] In particular, such an approach allows the powers of the state authorities to access personal data to remain unhindered.[70]

The above considerations confirm that the approach to data protection amounts to another manifestation of the peculiar Chinese nature. State organs are de facto excluded from the qualification as data controllers[71]. As a result, changes to the legislation were made while the status quo of state bodies was maintained.[72] It is a glaring example of the incompleteness of Chinese law, whether intended or not. The consequences of promoting and accepting such an approach hit the data subject first. It leads to a situation where the same processing activities undertaken by a state authority and a private sector entity entail different obligations and remarkably different restrictions, if any at all. Also, doubts regarding the qualification of any entity processing personal data as a data controller mean that the data subject does not know what is happening with their data. That is a severe problem because, the data controller is another leading actor in the processing of personal data. Specific obligations are imposed on the controller, who should

[68] Allen-Ebrahimian, B. (2022) China makes genetic data a national resource. *Axios*. 29 May. Available from https://www.axios.com/2022/03/29/china-makes-genetics-data-national-resource [accessed 30 November 2023].

[69] Greenleaf, G. (2020) China issues a comprehensive draft data privacy law. *Privacy Laws & Business International Report*, 1, p. 12.

[70] Gold, A. (2021) China's new privacy law leaves U.S. behind. *Axios*. 23 November. Available from: https://www.axios.com/2021/11/23/china-privacy-law-leaves-us-behind [accessed 30 March 2023].

[71] Creemers, R. (2021) China's Emerging Data Protection Framework. *Journal of Cybersecurity*, 8(1), p. 19.; Chen, Y-J., Lin C-F., Liu H-W. (2018) "Rule of Trust": The Power and Perils of China's Social Credit Megaproject. *Columbia Journal of Asian Law*, 32(1), p. 27; Duan, Y. (2019) Balancing the Free Flow of Information and Personal Data Protection. 3 April. Available from: https://ssrn.com/abstract=3484713 [accessed 26 April 2023], p. 11–12; Yu L., Ahl B. (2021) China's Evolving Data Protection Law and the Financial Credit Information System: Court Practice and Suggestions for Legislative Reform. *Journal Hong Kong Law Journal*, 51(1), p. 292

[72] Gold, A. (2021) China's new privacy law leaves U.S. behind. *Axios*. 23 November. Available from: https://www.axios.com/2021/11/23/china-privacy-law-leaves-us-behind [accessed 30 March 2023]; Yang, Z. (2022) The Chinese surveillance state proves that the idea of privacy is more "malleable" than you'd expect. *MIT Technology Review*. 10 October. Available from: https://www.technologyreview.com/2022/10/10/1060982/china-pandemic-cameras-surveillance-state-book/[accessed 28 March 2023].

handle the data appropriately. Moreover, the data controller is the addressee of the data subject's requests or complaints. Thus, if an entity that processes personal data, having defined the purposes and means of their processing, may not be considered
a controller, then such a legal system provides at least illusory protection of personal data. Therefore, the lack of clarity regarding the qualifications of state authorities as data controllers significantly reduce the level of personal data protection resulting from the entirety of Chinese law.

5. (NO) DATA AUTHORITY IN CHINA

As already mentioned, for EU law, the theoretical protection of personal data is less relevant than its actual level. Thus, a vital element of any third country's data protection regime should be adequate compliance supervision carried out by a supervisory authority. The provisions of the GDPR indicate that it is not about any public authority. It should be a body equipped with appropriate powers and resources. Moreover, the independence of such a body in performing the tasks entrusted to it must be guaranteed. However, it is difficult to say that such a supervisory authority has been established by Chinese law.

The Cybersecurity Law, Data Security Law, and Personal Information Protection Law devote some provisions to the supervision carried out by the supervisory authority. However, they operate with highly general terms, making identifying the entity considered a supervisory authority challenging.[73] The implication of the construction adopted is that there is a multi-stakeholder supervisory authority in China.[74] In other words, the functions of the supervisory authority are performed by various authorities. Consequently, there is no single, dedicated, specialised data protection authority. Instead, there are several public authorities in China. Among the tasks carried out by these authorities is the supervision of personal data protection, although this is not their primary task.[75] Such bodies include the Cyberspace Administration of China, the People's Bank of China, the

[73] Creemers, R. (2021) China's Emerging Data Protection Framework. *Journal of Cybersecurity*, 8(1), p. 14.

[74] Dorwart, H. (2021) Platform regulation from the bottom up: Judicial redress in the United States and China. *Policy & Internet*, 14(2), p. 383.; Liu, Y. et al. (2022) Privacy in AI and the IoT: The privacy concerns of smart speaker users and the Personal Information Protection Law in China. *Telecommunications Policy*, 46(7), p. 6–7.; Yin, Y. (2023) Conflict and Balance Between Private Information Protection and Public Interests Against the Background of Normalization of Epidemic Prevention and Control. *Hebei Law Science*, 3.

[75] You, C. (2022) Half a loaf is better than none: The new data protection regime for China's platform economy. *Computer Law & Security Review*, 45,,p. 22.

Ministry of Industry and Information, Technology and the Ministry of Public Security.[76]

The Cyberspace Administration of China is mostly identified as the data protection authority in China. This comes from the fact that a significant part of the powers or duties are addressed precisely to the entity identified as the Cyberspace Administration of China.[77] Nevertheless, this does not alter the fact that its jurisdiction is much broader, as it concerns network security issues.[78] Furthermore, doubts about recognising the Cyberspace Administration of China as a GDPR-compliant supervisory authority in China are compounded by its position towards other state authorities. The existing relationship prevents the Cyberspace Administration of China from being granted the characteristic of independence. It is pointed out that data protection-related institutions in China are closely linked to the state apparatus, including the political one.[79] As Creemers and You explain, despite the separation of the Cyberspace Administration of China from the State Council, it is still not clear that the Cyberspace Administration of China is an independent body.[80] Hence, multi-agency supervision would not be a problem as long as we could attribute the feature of independence[81] to each of these authorities. Independence guarantees that the authority will perform the tasks imposed on it freely, supervising all the other entities. Moreover, its actions will be based on objective criteria, detached from political preferences or suggestions from other authorities.

The most vivid example of politically driven action by the Cyberspace Administration of China is the case of DiDI Chuxing Technology. Under the cover of data-protection-related control, the Cyberspace Administration of

[76] Greenleaf, G., Livingston, S. (2016) China's New Cybersecurity Law – Also a Data Privacy Law? *Privacy Laws & Business International Report*, 144, p. 8.; Creemers, R. (2021) China's Emerging Data Protection Framework. *Journal of Cybersecurity*, 8(1), p. 10.; Chaskes, W. (2022) The Three Laws: The Chinese Communist Party Throws down the Data Regulation Gauntlet. *Washington and Lee Law Review*, 79(3), p. 1175.; Wang, C. et al. (2022 Privacy Protection in Using Artificial Intelligence for Healthcare: Chinese Regulation in Comparative Perspective. *Healthcare*, 10(10), p. 4.; You, C. (2022) Half a loaf is better than none: The new data protection regime for China's platform economy. *Computer Law & Security Review*, 45, p. 21.

[77] Creemers. R. (2021) China's Emerging Data Protection Framework. *Journal of Cybersecurity*, 8(1), p. 14.

[78] Dorwart, H. (2021) Platform regulation from the bottom up: Judicial redress in the United States and China. *Policy & Internet*, 14(2), p. 383–384.

[79] Pyo, G. (2021) An Alternate Vision: China's Cybersecurity Law and Its Implementation in the Chinese Courts. *Columbia Journal of Transnational Law*, 60(1), p. 236.

[80] You, C. (2022) Half a loaf is better than none: The new data protection regime for China's platform economy. *Computer Law & Security Review*, 45, p. 21.; Creemers, R. (2021) China's Emerging Data Protection Framework. *Journal of Cybersecurity*, 8(1), p. 14.

[81] Mentioned in the GDPR and indicated by the adequacy standard.

China pursued the state's goal of stopping DiDi's preparation of an initial public offering on the New York Stock Exchange against the state's will.[82]

Therefore, since one cannot speak of the independence of the state authorities to which the Cybersecurity Law, Data Security Law and Personal Information Protection Law address specific obligations, no competent supervisory authority can be said to exist in China. The systemic position of the supervisory authority in China raises the issue of the powers granted to the authority. The provisions of the Personal Information Protection Law (and, at times, the Cybersecurity Law, and the Data Security Law) do not deviate significantly from the catalogue of powers referred to in Articles 57 and 58 of the GDPR. Unfortunately, even the most advanced powers lose their meaning when it is unclear who would exercise them and when.

6. CONCLUDING REMARKS

hina's reformed data protection legislation has attracted the attention of many commentators. Without a doubt, the changes introduced can be described as advanced, considering the state of legislation before the Cybersecurity Law entered into force. However, there is no cause for excessive optimism, as has been proven by the three features of Chinese data protection law.

When it comes to the complicated structure of Chinese data protection legislation, the effect of the reform is to fundamentally deepen its existing fragmentation. The doctrine is unconvinced on how to treat the Cybersecurity Law, Data Security Law and Personal Information Protection Law. Some authors claim these laws are regulations of cyberspace and its safety, rather than personal data protection.[83] At the same time, others see the Personal Information Protection Law in particular as being a GDPR-like law or containing some GDPR-derived similarities.[84] Evidently,

[82] See among others: DigiChina (2022) Chinese Authorities Announce $1.2B Fine in DiDi Case, Describe 'Despicable' Data Abuses. *DigiChina*, 21 July. Available from https://digichina.stanford.edu/work/translation-chinese-authorities-announce-2b-fine-in-didi-case-describe-despicable-data-abuses/ [accessed 14. 11. 2023]; Dou, E., Wu, P.-L. (2022) China fines Didi $1.2 billion for breaking data-security laws. *The Washington Post*, 21 July. Available from: https://www.washingtonpost.com/world/2022/07/21/china-didi-fine-data-security/; Huld, A. (2022) How Did Didi Run Afoul of China's Cybersecurity Regulators? Understanding the US$1.2 Billion Fine. *China Briefing*, 2 August. Available from: https://www.china-briefing.com/news/didi-cyber-security-review-which-laws-did-didi-break/

[83] Liu, Y. et al. (2022) Privacy in AI and the IoT: The privacy concerns of smart speaker users and the Personal Information Protection Law in China. *Telecommunications Policy*, 46(7),, p. 12.; You, C. (2022) Half a loaf is better than none: The new data protection regime for China's platform economy. *Computer Law & Security Review*, 45, p. 24.

[84] Zheng, W. (2020) Comparative Study on the Legal Regulation of a Cross-Border Flow of Personal Data and Its Inspiration to China. *Frontiers of Law in China*, 15(3), p. 7; Pyo, G.

the Cybersecurity Law, the Civil Code, the Data Security Law, and the Personal Information Protection Law have been added to the sectoral regulations.

Such an unclear structure of Chinese data protection law weakens the protection it provides. The main consequence is that neither the data subject, nor the data controller or data processor are in a certain position. The data controller and the data processor will not find out whether they have applied the data protection legislation properly until one of authorities decides to check their activity. The same is true for data subjects, but here the convoluted relations within Chinese data protection law also becomes an opportunity to refuse the data subject's request by claiming it is based on the wrong law.

Another reason for finding the Chinese data protection law to be problematic is the status of state bodies. This is primarily influenced by the fact that the scope of the provisions of data protection law can easily be contested when it comes to state bodies. Moreover, even acknowledging with absolute certainty that the provisions in question apply and the state body is a data controller, this does not mean that the expected interpretation will prevail. As long as there is a state authority on the other side, the data subject should not count on being in the same situation as if a private sector entity had processed their data.

Lastly, there is also no dedicated data protection authority in China. It cannot be said that there is any competent supervisory authority in China, bearing in mind the standard of supervision set out in the GDPR. Instead, there are several bodies for which data protection is just an additional task. The functional shape of data protection supervision does not improve the situation, and nor did politically driven supervisory actions carry out recently.

With all this in mind, and even without considering the aspects of human rights protection in China that also affect personal data protection, as mentioned above,[85] I fall firmly into the part of the doctrine that considers the protection of personal data provided by Chinese law, including the Cybersecurity Law, the Civil Code, the Data Security Law, and the Personal

(2021) An Alternate Vision: China's Cybersecurity Law and Its Implementation in the Chinese Courts. *Columbia Journal of Transnational Law*, 60(1), p. 232; Calzada, I. (2022) Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL). *Smart Cities*, 5(3), p. 1130, 1140.; You. C (2022) Half a loaf is better than none: The new data protection regime for China's platform economy. *Computer Law & Security Review*, 45, p. 12.; Xixin, W. (2022) The Bundle of Personal Information Rights from the Perspective of State Protection. *Social Sciences in China*, 43(2), p. 47–48.

[85] Of course, bearing in mind the fact that a profound obstacle for China to be found adequate under the GDPR is its attitude towards human rights protection.

Information Protection Law, to be a long way short of the standard of adequacy under the GDPR.

LIST OF REFERENCES

[1] Allen-Ebrahimian, B. (2022) China makes genetic data a national resource. Axios. 29 May. Available from https://www.axios.com/2022/03/29/china-makes-genetics-data-national-resource [accessed 30 November 2023].

[2] Article 29 Working Party (1998) Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive (WP12, 24 July 1998),

[3] Belli L., Doneda D. (2023) Data protection in the BRICS countries: legal interoperability through innovative practices and convergence. International Data Privacy Law, 13 (1).

[4] Berti, R. (2020) Data Protection Law: A Comparison of the Latest Legal Developments in China and European Union. European Journal of Privacy Law & Technologies, 1.

[5] Blackmore N. (2019) Feeling inadequate? Why adequacy decisions are rare (and may get rarer) in Asia-Pacific. Kennedys 26 March, Available from: https://kennedyslaw.com/thought-leadership/article/feeling-inadequate-why-adequacy-decisions-are-rare-and-may-get-rarer-in-asia-pacific/[accessed 17 October 2022].

[6] Blume P. (2015) EU Adequacy Decisions: The Proposed New Possibilities. International Data Privacy Law, 5(1).

[7] Blume, P. (2000) Transborder Data Flow: Is There a Solution in Sight. International Journal of Law and Information Technology, 8(1).

[8] Bradford L., Aboy M., Liddell K. (2021) Standard Contractual Clauses for Cross-Border Transfers of Health Data after Schrems II. Journal of Law and the Biosciences, 8 (1).

[9] Cai P., Chen L. (2022) Demystifying data law in China: a unified regime of tomorrow. International Data Privacy Law, 12(2).

[10] Chen, J. Sun, J. (2021) Understanding the Chinese Data Security Law. International Cybersecurity Law Review, 2.

[11] Cai, P., Chen, L. (2022) Demystifying data law in China: a unified regime of tomorrow.

[12] International Data Privacy Law, 12(2).

[13] Calzada, I. (2022) Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL). Smart Cities, 5(3).

[14] Chaskes W. (2022) The Three Laws: The Chinese Communist Party Throws down the Data Regulation Gauntlet. Washington and Lee Law Review, 79(3).

[15] Chen, Y-J., Lin C-F., Liu H-W. (2018) "Rule of Trust": The Power and Perils of China's Social Credit Megaproject. Columbia Journal of Asian Law, 32(1).

[16] Creemers, R. (2021) China's Emerging Data Protection Framework. Journal of Cybersecurity, 8(1).

[17] Zhao, B., Feng, Y. (2021) Mapping the development of China's data protection law: Major actors, core values, and shifting power relations. Computer Law & Security Review, 40.

[18] Czerniawski, M. (2021) Rola Komitetu Art. 93 RODO w procedurze oceny adekwatności państw trzecich. Gdańskie Studia Prawnicze, 25(4).

[19] de Hert, P. Papakonstantinou, V. (2015) The data protection regime in China. In-depth analysis. European Union, Available from: https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA%282015%29536472_EN.pdf

[20] DigiChina (2022) Chinese Authorities Announce $1.2B Fine in DiDi Case, Describe 'Despicable' Data Abuses. DigiChina, 21 July. Available from https://digichina.stanford.edu/work/translation-chinese-authorities-announce-2b-fine-in-didi-case-describe-despicable-data-abuses/ [accessed 14. 11. 2023].

[21] Dorwart H. (2021) Platform Regulation from the Bottom up: Judicial Redress in the United States and China. Policy & Internet, 14(2).

[22] Dou, E., Wu, P.-L. (2022) China fines Didi $1.2 billion for breaking data-security laws. The Washington Post, 21 July. Available from: https://www.washingtonpost.com/world/2022/07/21/china-didi-fine-data-security/

[23] Drechsler, L., Kamara, I. (2022) Essential equivalence as a benchmark for international data transfers after Schrems II. In: Eleni Kosta, Ronald Leenes, Irene Kamara (eds.). Research Handbook on EU Data Protection Law. Edward Elgar Publishing.

[24] Duan, Y. (2019) Balancing the Free Flow of Information and Personal Data Protection. 3 April. Available from: https://ssrn.com/abstract=3484713 [accessed 26 April 2023].

[25] Duoye, X. (2020) The Civil Code and the Private Law Protection of Personal Information. Tsinghua China Law Review, 13(1).

[26] European Commission Communication (2013) Rebuilding Trust in EU-US Data Flows. COM 846 final, 23 November. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013DC0846.

[27] European Data Protection Board (2017) Adequacy Referential (WP 254 Rev.01, 28 November 2017).

[28] European Data Protection Board (2020) Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

[29] Feng, Y. (2019) The future of China's personal data protection law: challenges and prospects. Asia Pacific Law Review, 27 (1).

[30] Gao, R. Y. (2020) Personal Information Protection under Chinese Civil Code: A Newly Established Private Right in the Digital Era. Tsinghua China Law Review, 13(1).

[31] Gold, A. (2021) China's new privacy law leaves U.S. behind. Axios. 23 November. Available from: https://www.axios.com/2021/11/23/china-privacy-law-leaves-us-behind [accessed 30 March 2023].

[32] Greenleaf G. (2020) China issues a comprehensive draft data privacy law. Privacy Laws & Business International Report, 1.

[33] Greenleaf, G., Livingston, S. (2016) China's New Cybersecurity Law – Also a Data Privacy Law? Privacy Laws & Business International Report, 144.

[34] Guangping W. (2021) Challenges and Responses to the Protection of Workers' Personal Information in the Context of Human-Computer Interaction. China Legal Science, 9(139).

[35] Gulczyńska Z. (2021) A certain standard of protection for international transfers of personal data under the GDPR. International Data Privacy Law, 11(4). , A. (2022) How Did Didi Run Afoul of China's Cybersecurity Regulators? Understanding the US$1.2 Billion Fine. China Briefing, 2 August. Available from: https://www.china-briefing.com/news/didi-cyber-security-review-which-laws-did-didi-break/

[36] Judgement of 16 July 2020 Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559.

[37] Judgement of 6 October 2015 Maximillian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650.

[38] Kuner, C. (2009) Developing an Adequate Legal Framework for International Data Transfers. In: Serge Gutwirth, et al. (eds.). Reinventing Data Protection? Springer Science+Business Media B.V.

[39] Kuner, C. (2017) Reality and Illusion in EU Data Transfer Regulation Post Schrems. German Law Journal, 18 (4).

[40] Kuner, C. (2020) Article 44 GDPR. In: Christopher Kuner et al. (eds.). The EU General Data Protection Regulation (GDPR). A commentary. Oxford University Press.

[41] Kuner, C. (2020) Article 45 GDPR. In: Christopher Kuner et al. (eds.). The EU General Data Protection Regulation (GDPR). A commentary. Oxford University Press.

[42] Kuner, C. (2021) The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards. National Law Review of India, 33(1).

[43] Liu, J. (2020) China's data localization. Chinese Journal of Communication, 13 (1).

[44] Liu, Y. et al. (2022) Privacy in AI and the IoT: The privacy concerns of smart speaker users and the Personal Information Protection Law in China. Telecommunications Policy, 46(7).

[45] Makulilo, A. B. (2013) Data Protection Regimes in Africa: too far from the European 'adequacy' standard? International Data Privacy Law., 3(1).

[46] Panek, W (2024): The European Commission's adequacy decisions' content as a guide for applying the adequacy assessment criteria. The paper awaits publication in the Privacy Symposium Proceedings 2024 (Springer).

[47] Pernot-Leplay, E. (2020) China's Approach on Data Privacy Law: A Third Way between the U.S. and the EU? Penn State Journal of Law and International Affairs, 8(1).

[48] Pyo, G. (2021) An Alternate Vision: China's Cybersecurity Law and Its Implementation in the Chinese Courts. Columbia Journal of Transnational Law, 60(1).

[49] Qi, A., Shao, G., Zheng, W. (2018) Assessing China's Cybersecurity Law. Computer Law & Security Review: The International Journal of Technology Law and Practice, 34(6).

[50] Resolution of European Parliament (2016) Transatlantic data flows. Official Journal (C 76/82) 26 May. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016IP0233;

[51] Roth P. (2017) Adequate level of data protection' in third countries post-Schrems and under the General Data Protection Regulation. Journal of Law, Information and Science, 25(1).

[52] Schantz, P. (2023) Article 44 GDPR. In: Spiecker gen. Döhmann et al. (eds.). General Data Protection Regulation: Article-by-Article Commentary. Nomos.

[53] Schwartz P.M. (1995) European Data Protection Law and Restrictions on International Data Flows. Iowa Law Review, 80(3).

[54] Shao, Y. (2021) Personal Information Protection: China's Path Choice. US-China Law Review, 18 (5).

[55] Tene, O.(2022) Data transfer theatre: The US and Israel take the stage. Privacy Perspectives, 4 October, available from: https://iapp.org/news/a/

data-transfer-theater-the-us-and-israel-take-the-stage/ [accessed 17 October 2022].

[56] Tiwari, A. (2022) The Comparison between Indian Personnel and PRC New Civil Code, Cyber Laws, and Privacy. Jus Corpus Law Journal, 3.

[57] Trakman, L., Walters, R., Zeller, B. (2020) Digital consent and data protection law – Europe and Asia-Pacific experience. Information & Communications Technology Law, 29 (2).

[58] Vecellio Segate, R. (2020) Litigating Trade Secrets in China: An Imminent Pivot to Cybersecurity? Journal of Intellectual Property Law & Practice, 15(8).

[59] Wang Han S., Munir A.B. (2018) Information Security Technology – Personal Information Security Specification: China's Version of the GDPR? European Data Protection Law Review, (4) 4.

[60] Wang, C. et al. (2022) Privacy Protection in Using Artificial Intelligence for Healthcare: Chinese Regulation in Comparative Perspective. Healthcare, 10(10).

[61] Wittershagen, L. (2023) Transfer of Personal Data to Third Countries under the European Data Protection Law. In: Leonie Wittershagen (ed.) The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit. De Gruyter.

[62] Wolf C. (2013) Delusions of Adequacy - Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers. Washington University Journal of Law & Policy, 43.

[63] Xing H. (2023) Government Data Sharing and Personal Information Protection. Administrative Law Research, 2.

[64] Zhou Q. (2023) Whose data is it anyway? An empirical analysis of online contracting for personal information in China. Asia Pacific Law Review, 31 (1).

[65] Xixin, W. (2022) The Bundle of Personal Information Rights from the Perspective of State Protection. Social Sciences in China, 43(2).

[66] Yablonko, Y. (2020) Israel's outdated privacy laws jeopardize relations with EU. Globes, 23 July, available from: https://en.globes.co.il/en/article-israels-outdated-privacy-laws-jeopardize-relations-with-eu-1001337077 [accessed 17 October 2022].

[67] Yan Wang, C. (2022) Governing Data Markets in China: From Competition Litigation and Government Regulation to Legislative Ordering. George Mason International Law Journal. 13(1).

[68] Yang, Z. (2022) The Chinese surveillance state proves that the idea of privacy is more "malleable" than you'd expect. MIT Technology Review. 10 October. Available from: https://www.technologyreview.com/2022/

10/10/1060982/china-pandemic-cameras-surveillance-state-book/[accessed 28 March 2023].

[69] Yin, Y. (2023) Conflict and Balance Between Private Information Protection and Public Interests Against the Background of Normalization of Epidemic Prevention and Control. Hebei Law Science, 3.

[70] You, C. (2022) Half a loaf is better than none: The new data protection regime for China's platform economy. Computer Law & Security Review, 45.

[71] Yu L., Ahl B. (2021) China's Evolving Data Protection Law and the Financial Credit Information System: Court Practice and Suggestions for Legislative Reform. Journal Hong Kong Law Journal, 51(1).

[72] Yuexin, Z. (2019) Cyber Protection of Personal Information in a Multi-Layered System. Tsinghua China Law Review, 12(1).

[73] Zhao, B. (2021) Connected Cars in China: Technology, Data Protection and Regulatory Responses. In: Alexander Roßnagel, Gerrit Hornung (eds.). Grundrechtsschutz im Smart Car. DuD-Fachbeiträge. Wiesbaden: Springer Vieweg.

[74] Zhao, B., Feng, Y. Mapping the development of China's data protection law: Major actors, core values, and shifting power relations. Computer Law & Security Review, 40.

[75] Zheng, G. (2021) Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S. and China. Computer Law & Security Review, 43.

[76] Zheng, W. (2020) Comparative Study on the Legal Regulation of a Cross-Border Flow of Personal Data and Its Inspiration to China. Frontiers of Law in China, 15(3).

[77] 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] (issued by the Standing Committee of the National People's Congress on 20 August 2021, came into force on 1 November 2021, bilingual version accessed via PKU Law database).

[78] Zhonghua Renmin Gongheguo Minfa Dian (中华人民共和国民法典) [Civil Code of of the People's Republic of China] (issued by the National People's Congress on 28 May 2020, came into force on 1 January 2021, bilingual version accessed via PKU Law database)

[79] Zhonghua Renmin Gongheguo shuju Anquan Fa (中华人民共和国数据安全法) [Data Security Law of the People's Republic of China] (issued by the Standing Committee of the National People's Congress on 10 June 2021, came into force on 1 September 2021, bilingual version accessed via PKU Law database).

[80] Zhonghua Renmin Gonghegup Wanglup Anquan Fa (中华人民共和国网络安全法) [Cybersecurity Law of the People's Republic of China] (issued by the Standing Committee of the National People's Congress on 11 July 2016, came into force on 1 June 2017, bilingual version accessed via PKU Law database).

[81] Zhou, Q. (2023) Whose data is it anyway? An empirical analysis of online contracting for personal information in China. Asia Pacific Law Review, 31 (1).