Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 6 (2023)

Which are the Legal Issues Surrounding Data Privacy in Internet Courts?

Carolina Fabara [1]

[1] *PhD (c) Chinese University of Political Science and Law*

Abstract:- The legal issues surrounding data privacy in the context of Internet Court are complex and multifaceted. Some of the major legal issues include massive collection of personal data, privacy and transparency in data processing. The Internet Courts present data privacy issues because data providers secure the informed consent of digital consumers before accessing and transmitting their personal data. Additionally, the use of AI in Chinese courts raises concerns about privacy and data protection, as the collection and processing of sensitive information may be susceptible to vulnerabilities. The lack of clarity in data protection laws and the possibility that AI could access sensitive information is an important issue for data privacy. In China, three major laws constitute the legal framework regarding cyber security, data sovereignty, and personal information protection, that is, the Cybersecurity Law (CSL), Data Security Law (DSL), and Personal Information Protection Law (PIPL). However, despite these regulatory efforts, there are still legal gaps related to the data privacy consent of Internet Courts users, the use of AI in courts and the technology companies working in the creation of the new judicial system. Therefore, this paper will address the question of which are the legal issues surrounding data privacy in the Internet Courts, by addressing the impact in data protection, the laws and regulations and the legal loopholes around data privacy in China.

Keywords*: data protection, China legal framework, data privacy, Smart Court, AI in Judicial system.*

1. New Information Technologies and Artificial Intelligence

The new information technologies open the door to legal loopholes in the area of data privacy. The new judicial system in China also bring to the table some questions around how the personal data will be treated in the Internet Courts and how the different networks will proceed. The use of AI in Internet Court raises data privacy concerns. The legal issues surrounding data privacy in Internet Courts are still evolving and the best practices for protecting sensitive information are still being developed.

The urgent need for transnational standards for personality and data protection rights on the one hand, while on the other hand reach a consensus on such standards, given the diverse legal cultures in the regions of the world. Moreover, an economic dilemma for Internet regulators is to recognize the economic costs to data providers of informing data consumers about the nature and consequences of consenting to the use of their personal data, while preventing data users from eroding the privacy of those consumers. This all is reflected in China unique way of constructing Internet Courts system. This new system are embedded in China’s larger strategy of capturing new opportunities offered by the information and communications technology (ICT) revolution (Zheng 2020). The success of online litigation via the Internet Court as a new type of technology enabled dispute resolution, reflects a new governance approach with a dynamic interaction between the State, the market, and technology.

In China, in the case of Internet users the data users are process as the laws and regulation mentioned. For instance, China’s Cybersecurity Law does require both the notification and consent of data users whose personal information is collected by providers of network products and services. Specifically, Article 22 of the Cybersecurity Law provides that network products and services shall comply with the compulsory requirements of relevant national standards. Providers of network products and services shall not install malware (Liu et al. 2022). When a provider discovers any risk, such as security defect and vulnerability of its network products or services, it shall immediately take remedial measures, inform users in a timely manner, and report the defect or vulnerability to the competent department in accordance with relevant provisions. (Liu et al. 2022). Where network products and services have the function of collecting users' information, their providers shall explicitly notify their users and obtain their consent. If any user's personal information is involved, the provider shall also comply with this law and the provisions of relevant laws and administrative regulations on the protection of personal information.

China law focuses on regulating data use and collection by government and business. Additionally, China law focuses on information such as names, addresses and identification numbers. It is important to mention that every law protect individual personal data, but have different approaches and regulations. A notable difference from the consent to the use of personal data in the EU and Australia is that the term consent is only used once in China Cybersecurity Act. The Act does not define consent, nor describe how and what it might constitute. China is attempting to provide a minimum level of consent where a network or other service collects information, whether personal or otherwise. The Cybersecurity Act does provide that the data subject must be notified and must consent to that use. However, the nature of that consent is not defined in that Act. There is also no mention of protecting the personal data of vulnerable sectors of society, such as the protection of minors, unlike the EU and Australia that provide for such protection (Trakman, Walters, and Zeller 2020). Every country such as EU, the United States, Australia, has their own legislation and data privacy has their own concept and way to be regulated.

The Internet Courts incorporate technologies to promote the judiciary efficiency and transparency. On 26 June 2017, the Central Commission of Comprehensively Deepening Reform adopted the Planning for Establishing the Hangzhou Internet Court. The first Internet Court was launched on 18 August 2017 in the City of Hangzhou, which is dubbed the "capital of Chinese E-commerce" due to hosting Alibaba technology companies. In 2018, the Internet Court was also established in Beijing and Guangzhou (Zheng 2020). The question is how this new way of legal system affect privacy and individual rights in the context of artificial intelligence in the judicial field.

Since Internet Courts is used in China as a new judicial method, where the data privacy is an important topic that involve the consent of the user to use their data. Furthermore, the technology of artificial intelligence is part of this evolution in the judicial system and involve some concerns around the way data is being threated. In recent years, consumer markets have increasingly been shaped by new information technologies and artificial intelligence (AI) systems. Progress in AI technology has brought novel experiences in many fields and has profoundly changed industrial production, social governance, public services, business marketing, and consumer experience (Lagioia et al. 2022). A number of AI technology products or services have been successfully produced in the fields of industrial intelligence, smart cities, self-driving cars, smart courts, intelligent recommendations, facial recognition applications, smart investment consultants, and intelligent robots. At the same time, the risks of fairness, transparency, and stability of AI have also posed widespread concerns among regulators and the public (Shen and Liu 2022). This also works for the legal system that could use AI technology to help solve disputes without requiring lawyers or the traditional court system (Soares 2020). The development and use of AI for the provision of legal services is limited with regard to three main aspects, namely (1) data; (2) algorithms; and (3) implementation. Data are a critical part of AI systems as both training material for developing AI algorithms and input material for the actual use of AI. The development and use of AI algorithms in the provision of legal services is limited by a lack of easily accessible and analyzable datasets. Therefore, data privacy and cybersecurity concerns also arise with the use of massive quantities of data by AI systems.

Legal loopholes and data privacy for users in Internet Courts are constantly evolving and may vary by jurisdiction. In general, Internet Courts are designed to handle legal disputes that arise online, and data privacy is a crucial aspect. Depending on the country and applicable laws, foreign users may face additional challenges in relation to the protection of their personal data in online legal proceedings. Having in mind that in China in the Internet Courts are assisted by AI. Therefore, it is important to talk about the impact in data protection.

2. Impact in Data Protection

Data is the key factor driving the prosperous development of a new generation of AI. The Cyber Security Law enacted in November 2016 sets requirements for the security of important data and personal information respectively, and AI developers must comply with relevant regulations when processing data. In particular, national security and public interest should be safeguarded when dealing with important data, and the rights and interests of natural persons should be protected when dealing with personal information (Bu 2020). The problem is that this definition of personal data or personal information can vary from country to country.

China does not define personal data or personal information or sensitive personal data. The only reference to personal information is contained in Article 22 of China's Cybersecurity Act. It states that, where network products and services have the function of collecting users' information, their providers shall explicitly notify their users and obtain their consent. If any user's personal information is involved, the provider shall also comply with this Cybersecurity law and the provisions of relevant laws and administrative regulations on the protection of personal information. Notwithstanding the absence of a definition of personal data, China does identify with the protection of personal data through networks systems and data platforms, over and above the individual data subject (Trakman, Walters, and Zeller 2020). Consequently, it is possible to said that the law focus more on the collection and legitimate use of personal data.

In this sense companies must ensure that personal data collected and processed in the context of online courts is protected in accordance with applicable data privacy law. Also, they must obtain informed consent from the parties involved in online court cases to collect, process and store their personal data. Companies must implement appropriate security measures to protect confidential information handled in online courts and prevent unauthorized access. If data is transferred between jurisdictions, companies must comply with laws and regulations on international data transfer, such as the EU-US Privacy Shield. Therefore, it is important to understand the different concepts that are used in the legislation of each country.

3. Privacy, Personal Data, and Personal Information Protection

It is necessary to clarify the concepts concerning privacy, personal data and personal information. Justice Cooley initially defined privacy as "the right to be left alone" in 1888. Despite the meaning of privacy having evolved over time, there is no consensus regarding its definition (Nissim and Wood 2018) (Shi, Winter, and Zhang 2021) mentioned that the term privacy has frequently been included in U.S. laws and regulations when concerned with personal information, but its counterpart, data protection, is often used in other countries or regions, such as in the EU. (Liu et al. 2022) This concept and definitions varies in every country.

China's data protection laws make a clear distinction between privacy and personal information. In the Civil Code of the People's Republic of China (the Civil Code), privacy is defined as "the private peace of mind of a natural person and the private space, private activities, and private information that he or she does not want others to know about" (Article 1032). The Personal Information Protection Law (PIPL) defines "personal information" as "all kinds of information related to identified or identifiable natural persons that are electronically or otherwise recorded, excluding information that has been anonymized" (Article 4). To some extent, the term "personal information" in China's legislation corresponds to the definition of personal data in the European Union`s General Data Protection Regulation (GDPR), but there are subtle distinctions in the approach to defining information/data recording (Shao and Huang 2021). It is important to mention that PILP is China`s comprehensive privacy law and bear resemblance to the GDPR. Taking in account that in China personal data is any information relating to an identified or identifiable person.

The law in China focuses on protecting the legitimate rights and interests of citizens and organizations, and promoting socioeconomic development. Consequently, in China there is different authorities responsible for supervising and regulating the use of Internet and data privacy. For instance, the Ministry of Industry and Information Technology (MIIT) is mainly responsible for industrial planning, policies and standards. As for the standard setting, the MIIT often collaborates with the Standardization Administration of China (SAC). The Ministry of Public Security (MOPS) and the Cyberspace Administration of China (CAC) are entitled to handle online information security infringements (Ermakova 2023). Since multiple government agencies are involved with personal information protection and their responsibilities are overlapping, some scholars have criticized this phenomenon mentioned at (Thoughts on personal information protection supervision. strategies in the digital development era. *Information and Communications Technology and Policy),* by (Quan & Liu, 2021). They have been calling for establishing a unified regulatory body in order to clarify law enforcement responsibilities.

However, it is important to mention that in China the private technology companies have unique collaboration in the process of establishing the Internet Courts.

4. Private Technology Companies Involved in Internet Courts Process

The rapid growth of online dispute settlement on e-commerce platforms in Chine should be treated with caution. Online dispute settlement (ODS) on the platforms has changed the traditional concepts of justice. The broad use of ODS technologies in creating Internet courts in China has changed the relations in courts between practicing lawyers and contestants, transformed judicial results, and ultimately changed the overall experience of justice. Chinese experts emphasized that the political incentives leading to the more rapid introduction of ODS technologies in courts will continue to stress the positive aspects of ODS, including accessibility, efficiency, predictability and prevention of disputes (Ermakova 2023). The ODS also causes serious concerns with regard to the traditional principles of justice, such as objectivity, confidentiality and data safety in dispute settlement.

In 2019, PRC adopted the E-Commerce Law, which allowed e-commerce operators to create their own online systems for dispute settlement. In June 2021, the Supreme Court of PRC published the "Regulation of online court procedures of people's court", and in December of the same year amendments to the Civil-Procedural Code of PRC were adopted regarding the development of online hearings (Ermakova 2023). All normative acts were created based on the studies and summarization of the practice of dispute resolution on Chinese e-commerce platforms (2023). E-commerce platforms adopted from the state the authorities to ensure law observance within their competence; besides, they helped the state to create formal legislation, experimenting with the character and content of legal norms suitable for managing their platforms. [1]Therefore, the PRC government is not the only one striving for cooperation with private technological companies with a view of digital reforming of their legal system (Ermakova 2023). The Chinese government consulted with Alibaba about the design of the Internet court of Hangzhou. Besides, Alibaba company provides cloud services to the Internet court of Hangzhou. Alibaba company also created a means to transfer evidences to the Internet court from its e-commerce websites with a mouse click.

The Hangzhou Internet Court's online lawsuit platform, for example, is technically supported by the Alibaba Group. Meanwhile, Alibaba and its subsidiaries are related to many E-commerce disputes. Unsurprisingly there rise public doubts as to the impartiality of the operation of the Hangzhou Internet Court. This suspected compromise of judiciary impartiality, however, might be contained with the potential regulatory competition from other two Internet Courts (You and Bu 2020). Additionally, the use of cloud computing in Internet Courts can also raise concerns about data privacy, as it can lead to complex litigation and regulatory matters before courts and agencies such as in the United States, Europe or elsewhere. Motivations of these companies must be different from public institutions. Which means that the process need to be made accountable. Making sure that the data itself is not biased and the algorithms are fair is a fundamental challenge not only for China but for the whole world.

In 2019, a new project was introduced in the Internet court of Hangzhou, a pilot AI judge assistant (试点AI**助理法官**), also developed by Alibaba (You and Bu 2020). To illustrate, Alibaba, a Chinese e-commerce corporation and one of the biggest tech companies in the world, participated in the development of AI for online transaction disputes. This gives the idea of how the online process will be handle, additionally the AI technology is used in the new judicial process.

5. Internet Court Process: Limits of Automated Law

In China, people can use smartphones to file a complaint, track the progress of a case and communicate with judges. AI-based automated machines found in so called "one stop" stations provide legal consultations, register cases, and generate legal documents 24 hours a day. They can even calculate legal costs. However, there is a debate over the reliability of information provided by these automated lawyers. The Internet Courts undertake the entire process of litigation with the aid of the information communication technologies including the Internet, online streaming, facial recognition, etc(You and Bu 2020). Procedures including the filing of cases, service of documents, exchange of evidence, hearing of cases, and pronouncement of judgments are conducted via the specially designed multifunctional integrated online lawsuit platform(You and Bu 2020).The use of online hearings, face recognition and video recording in the Internet Court process raises several issues related to data privacy. The use of these technologies can lead to the collection and processing of personal data, which can be misused or leaked, leading to privacy violations.

All the information is supposed to be on the Internet, so what happen is that AI system make assessments based on an incomplete public record. The problem is that some cases are not yet online in some regions of China. Moreover, some controversial cases have been removed from the government database. This raised concerns about whether AI based on fragmented data can make unbiased decisions.

6. The Use of AI in China`s Smart Court

Data privacy issues in China`s internet courts using AI include concerns about the collection and use of personal data, information security during online court proceedings, and transparency in information handling of the users. One of the concerns is that AI system may have access to sensitive information, which could be vulnerable to data breaches, hacking and other security violations. In addition, there are concerns about the ethical implications of using AI to assist with more complicated legal decisions in cases where a decision made based on AI calculations may be deemed more credible than a decision made by human. Another issue is that AI systems make assessments based on an incomplete public record, due to the uneven digitization of China`s region.

In terms of legal regulation, China has implemented laws such as the Cybersecurity Law and the Personal Data Protection Law, which seek to address these concerns and establish guidelines for the use of AI in smart courts. Smart courts in China use AI to speed up court processes but this raises concerns about data privacy. To protect the privacy of data collected by AI in China`s smart courts, security measures such as data encryption, strict access control, and anonymization of personal information are implemented where possible. The legal regulations in China that address data protection and privacy are the Cyber Security Law and the Personal Data Protection Law. These laws establish requirements for the secure and legal handling of data, including that collected by AI systems in smart courts.

One of the basic principles for responsible AI is accountability, which also applies to data governance. The developers, controllers, and operators of AI systems can also be regarded as personal information processors on PIPL or data processors on Data Security Law, and they must comply with the above obligations. If the relevant obligators of the AI system violate data security obligations, they are liable for the corresponding damage consequences (Shen and Liu 2022). The effective Civil Code, E-Commerce Law, Product Quality Law, and other relevant legislations can serve as legal requirements developing responsible AI. In addition, new laws and other binding documents enacted in recent years provide a substantial basis for AI governance, and the effective and draft documents released show that responsible AI is increasingly a concrete goal that needs to be enforced. Consequently, is necessary to study the laws and regulations around Data Privacy in China.

7. Laws and Regulations Around Data Privacy

China has around 270 laws, regulations and rules concerned with the protection of personal information at Shao and Huang (2021). The provisions related to personal information protection are scattered across different laws and regulations. The 2016 Cybersecurity Law (CSL) is a landmark piece of legislation that focuses on the Internet safety issues within the territory of China and provides legal guidance to basic network operation (Parasol 2017). Network operators are obligated to publicly disclose their ways of data usage and obtain consent from users. (Liu et al. 2022). China has enacted the last year’s new laws and regulations that are important to have in mind.

The Cybersecurity Law of the People’s Republic of China, as adopted at the 24th Session of the Standing Committee of the Twelfth National People’s Congress of the People’s Republic of China on 7 November 2016, came into force on 1 June 2017. It must be noted that data protection law of China is quite different to other jurisdictions. One underlying reason for that difference is that the protection of personal data is secondary to the protection of networks, systems and platforms in China (2022). This is related with the scope of the law and the country standards.

The Cybersecurity Law divide the cyberspace into four parts and regulate each accordingly. These parts include: (1) the critical information infrastructure ("CII"), as the basic foundation, (2) the intermediate Internet platforms example the ecommerce platforms, (3) the Internet users, and (4) the cyber-data of the Internet users. The Cybersecurity Law is one of the foundational cyberspace legislation designated to regulate CII operators and operators of other network facilities. The Cybersecurity Law governs any individual or entity that "construct, operate, maintain or use any 'network' within China and the overall cybersecurity in China" (Liu et al. 2022). The definition of "network" and "network operators" are drafted broadly, and can cover telecommunication service providers such as Baidu, Alibaba, Tencent, and potentially all businesses operating in China since nearly all businesses administer computer networks at least for internal use (Ji 2018). In particular, this law establishes the regulatory frameworks and the protection of critical information.

In 2020, the newly released Civil Code of the People's Republic of China (Civil Code) protects privacy and personal information interests. The Civil Code confirms the civil right status of privacy and personal information. It provides a comprehensive illustration of privacy protection through Article 1032 and Article 1033. Article 1035 of the Civil Code expands the scope of information protection to all data-related activities, including storage, transmission, and publication (Chow 2021). Such a stipulation accommodates the data-centric nature of smart speakers and other human-computer interaction applications. In addition, the Civil Code enlarges the scope of obligators to all personal information processors, which strengthen the protection of individuals' rights in personal information(Cui and Qi 2021).Civil Code has laid down a 'privacy right' and a 'personal information right.' Privacy refers to a natural person's undisturbed private life and the private space, private activities, and private information that the person does not want others to know about, while personal information is recorded electronically or by other means that can be used, by itself or in combination with other information, to identify a natural person.

In June 2021, Data Security Law (DSL) was formally promulgated. It is recognized to be a vital block of the information protection's legal system, instead of simply an extension of the previous Cybersecurity Law (Dong, Guo, and Dong 2020). Although both laws underline national security and Internet sovereignty, the CSL has mainly focused on the overall robustness of cyberspace. The DSL calls for a specified data classification and the clarification of "important data" by regulatory administrations, districts, and industries. However, international data transfer behaviors for daily operational or business purposes will face prior assessment or export control. For public safety reasons, data processors that illegally transmit data abroad face penalties in the form of fines or even being closed. Since cloud storage is widely applied to smart devices to deal with huge amounts of user data, companies shall be alerted if their servers are located overseas or are simultaneously hosting global data (Liu et al. 2022). This law focuses on the protection of data security from a national security perspective.

In 2021, the Data Security Law and Personal Information Protection Law (PIPL) jointly provided for a more comprehensive approach to data governance. Responsible AI is ensured through new legal rules in four major dimensions in the field of data governance: giving individuals new civil rights, setting out obligations for processors, building a governance system for data security risk, and strengthening data processing responsibilities (Shen and Liu 2022). The new civil rights granted to individuals are mainly reflected in Chapter 4 of the PIPL.

Although there are the CSL, DSL, and other laws mentioned above dealing with personal information rights and protection, a separate law directly protecting personal information is still needed. The PIPL supplements the CSL and the DSL in legislation, forming a full-scale legal framework that fits in the Chinese context to ensure personal information protection and data security (Wu and Yao 2022). The PIPL serves as a fundamental law in the field of personal information protection, which reflects a high-level legal status in the Chinese legal system. The PIPL gives individuals more choices to control their personal information especially by complementing and optimizing their rights as data subjects. For example, it introduces a series of self-determination rights including the right to be informed, right to access, right to correct, the right of data portability (Liu et al. 2022). The primary legal basis under PIPL is consent and if consent is relied on the legal basis, a separate consent will be needed in specific cases.

China constructs the strict protection of privacy rights, protecting natural persons from being exposed or interfered with and giving them the right to keep personal information from being handled illegally. According to the Civil Code, the private information included in personal information shall apply to the provisions of privacy; if there is no such provision, the provisions on the protection of personal information, such as the PIPL, shall be applied. The PIPL provides a series of specific rights in Articles 44–55, the content of which is consistent with the connotation of some articles of the European Union (EU) General Data Protection Regulation (GDPR) (Shen and Liu 2022). Both laws aim to ensure respect for privacy and data security. However, the GDPR focuses on the user`s explicit consent for the processing of their personal data, while PIPL focuses on focuses on the collection and legitimate use of personal data. Every country has different approaches and legal frameworks regarding data privacy. In the case of China, its Cybersecurity Law and Personal Data Protection Law could be involved in regulating data privacy in Internet Courts. Meanwhile, in the United States, laws such as the California Online Consumer Privacy Act (CCPA) and the California Consumer Privacy Act (CPRA) could influence how data privacy is addressed in the United States. International collaboration and the adoption of common standards will likely be required to effectively address data privacy concerns in Internet Courts.

To sum up, there is no comprehensive legislative outcome, China's solutions for responsible AI can be extracted in all relevant laws. For example, the E-Commerce Law dictates prohibitions on the use of personal information for Big-Data Driven Price Discrimination, while the Cybersecurity Law, the Personal Information Protection Law and the Data Security Law these three fundamental laws set requirements in terms of automated decision-making rules and data security requirements but still some legal loopholes and uncertainty regarding the data privacy consent of Internet Courts users, the use of AI in courts and the technology companies working in the creation of the new judicial system, which bring to the table the question of this paper: Which are the legal issues surrounding data privacy in Internet Courts? The main reason is that different laws and regulations in China having different frameworks of data privacy can lead ambiguity and confusion. However, China is developing legal frameworks to address this issues such as the PIPL which is targeted at personal information protection and address the problems with personal data leakage. It is important to ensure that the use of the technology is in compliance with data privacy laws and regulations, and that appropriate safeguards are in place to protect the privacy of individual involved in the Internet Court process.

References

[1] Bu, Qingxiu. 2020. "Transformative Digital Economy, Responsive Regulatory Innovation and Contingent Network Effects: The Anatomy of E-Commerce Law in China." SSRN Scholarly Paper. Rochester, NY. https://papers.ssrn.com/abstract=3719874.

[2] Chow, Vicent. 2021. "China's Civil Code Expands Personal Information Protection, Strengthens Contractual Protections." China Law and Practice. December 3, 2021. https://www.chinalawandpractice.com/2020/12/03/chinas-civil-code-expands-personal-information-protection-strengthens-contractual-protections/.

[3] Cui, Shujie, and Peng Qi. 2021. "The Legal Construction of Personal Information Protection and Privacy under the Chinese Civil Code." *Computer Law & Security Review* 41 (July): 105560. https://doi.org/10.1016/j.clsr.2021.105560.

[4] Dong, Xiao, Jinghe Guo, and Junjie Dong. 2020. "Data Security Legislation Accelerated – Draft Data Security Law Released for Public Consultation." July 10, 2020. https://www.junhe.com/legal-updates/1252?locale=en.

[5] Ermakova, Elena P. 2023. "Features of Online Settlement of Consumer Disputes by E-Commerce Platforms in the People's Republic of China." *Journal of Digital Technologies and Law* 1 (eng) (3). https://cyberleninka.ru/article/n/features-of-online-settlement-of-consumer-disputes-by-e-commerce-platforms-in-the-people-s-republic-of-china.

[6] Ji, Chen. 2018. "Cybersecurity and Data Protection: A Study on China's New Cybersecurity Legal Regime and How It Affects Inbound Investment in China." *The International Lawyer* 51 (3): 537. https://scholar.smu.edu/til/vol51/iss3/6.

[7] Lagioia, F., A. Jabłonowska, R. Liepina, and K. Drazewski. 2022. "AI in Search of Unfairness in Consumer Contracts: The Terms of Service Landscape." *Journal of Consumer Policy* 45 (3): 481–536. https://doi.org/10.1007/s10603-022-09520-9.

[8] Liu, Yu-li, Luyan Huang, Wenjia Yan, Xinghan Wang, and Ruochen Zhang. 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). https://ideas.repec.org//a/eee/telpol/v46y2022i7s0308596122000362.html.

[9] Nissim, Kobbi, and Alexandra Wood. 2018. "Is Privacy Privacy?" *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376 (2128): 20170358. https://doi.org/10.1098/rsta.2017.0358.

[10] Parasol, Max. 2017. "The Impact of China's 2016 Cyber Security Law on Foreign Technology Firms, and on China's Big Data and Smart City Dreams." *Computer Law & Security Review* 34 (June). https://doi.org/10.1016/j.clsr.2017.05.022.

[11] Shao, Guosong, and Gi Huang. 2021. "Trends and Challenges of Global Convergence of Personal Data Protection." *Journal of Shanghai Jiaotong University(Philosophy and Social Sciences)*, 2021. https://kns.cnki.net/kcms/detail/detail.aspx?doi=10.13806/j.cnki.issn1008-7095.2021.04.012.

[12] Shen, Weixing, and Yun Liu. 2022. "China's Normative Systems for Responsible AI: From Soft Law to Hard Law." In *The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives*, edited by Oliver Mueller, Philipp Kellmeyer, Silja Voeneky, and Wolfram Burgard, 150–66. Cambridge Law Handbooks. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781009207898.012.

[13] Shi, Peilin, Jenifer Sunrise Winter, and Bin Zhang. 2021. "Governance of Privacy Protection: How Laws Will Be Adopted to Address New Technologies?" In . Calgary: International Telecommunications Society (ITS). https://www.econstor.eu/handle/10419/238053.

[14] Soares, Marcelo Negri. 2020. "AI in Legal Services: New Trends in AI-Enabled Legal Services." *Service Oriented Computing and Applications*, January. https://www.academia.edu/104729549/AI_in_legal_services_new_trends_in_AI_enabled_legal_services.

[15] Trakman, Leon, Robert Walters, and Bruno Zeller. 2020. "Digital Consent and Data Protection Law – Europe and Asia-Pacific Experience." *Information & Communications Technology Law* 29 (2): 218–49. https://doi.org/10.1080/13600834.2020.1726021.

[16] Wu, Victor, and Laura Yao. 2022. "Interpretation of the Personal Information Protection Law - Professional Articles - AllBright Law Offices." March 10, 2022. https://www.allbrightlaw.com/EN/10475/3946f862bac0e12c.aspx.

[17] You, Chuanman, and Qingxiu Bu. 2020. "Transformative Digital Economy, Responsive Regulatory Innovation and Contingent Network Effects: The Anatomy of e-Commerce Law in China," August. https://sussex.figshare.com/articles/journal_contribution/Transformative_digital_economy_responsive_regulatory_innovation_and_contingent_network_effects_the_anatomy_of_e-commerce_law_in_China/23306945/2.

[18] Zheng, George. 2020. "China's Grand Design of People's Smart Courts." *Asian Journal of Law and Society* 7 (November): 1–22. https://doi.org/10.1017/als.2020.20.