WEI DING*

THE MAKING OF DATA SECURITY LAW IN CHINA: FRAMEWORK, ISSUES AND FUTURE TRENDS

ABSTRACT: With the development of information technology, data security has become a hot issue of concern for all countries. Data security legislation and data governance have become an important legal guarantee for the steady and sustained development of the digital society. China's Data Security Law needs to balance the values of security and development, clarify the normativity and uniformity of the core categories of data, examine the legitimacy of state public power's involvement in data governance, and reasonably set up the review rules for cross-border data transfer. In the future, it is necessary to establish a data security legislative framework, give full play to the multiplier effect of data elements, benchmark international rules, optimise the regulatory measures for cross-border data flow, establish and improve the data security rule system in the field of artificial intelligence, and contribute Chinese wisdom to the establishment of an international data governance and global data rule system.

KEYWORDS: Data security, Data power, Artificial intelligence, Data security regulation

I. INTRODUCTION

With the rapid development of big data, the fluidity and resourcefulness of data are constantly enhanced.[1] Data security has become an unavoidable issue in the development of digital society, making human beings face

* This paper is the phased research result of the National Social Science Foundation Project "Research on Constitutional Regulation of Private Power in Digital Society" (21BFX043). Thanks to the support of the National Social Science Foundation.

[1] The Global Big Data Analytics Market was valued at US$ 37.34 billion in 2018 and expected to reach US$ 105.08 billion by 2027 at a CAGR of 12.3% throughout the forecast period from 2019 to 2027. Both an increasing volume of data and the adoption of big data tools to spur revenue growth are expected during the forecast period. See 'Global Big Data Analytics Market Size, Market Share, Application Analysis, Regional Outlook, Growth Trends, Key Players, Competitive Strategies and Forecasts, 2019 To 2027' (RESEARCH AND MARKETS) <https://www.researchandmarkets.com/> accessed 20 Feb 2024.

more risks and challenges. These challenges include but are not limited to personal information and privacy protection, excessive collection and use of sensitive data and personal data, leakage of business secrets of enterprises, global and systematic security problems caused by attacks on the Internet of Things and cloud computing related to big data, threats to economic security and social order from malicious data sources, slow progress in government data sharing and disclosure due to data security risks, data security and data sovereignty problems caused by cross-border data flow, etc. To this end, the United States has formulated the Open Government Data Act,[2] and the European Union has formulated the General Data Protection Regulation (GDPR)[3] and the European Strategy for Data.[4] While attaching importance to the development of the data industry and releasing data strategies, they have passed data security policies and legislation to protect data security and ensure the healthy development of digital society and economy. In this context, the Data Security Law of the People's Republic of China (hereinafter referred to as DSL) was officially implemented on September 1, 2021 after three rounds of deliberation. The DSL marks a major leap in China's process of data security and governance law, which has attracted wide attention from the world. The law fills the gap in China's data security legislation at the national level. Since then, China has issued a series of data-related policies and regulations, aimed at establishing and improving its data security norms system.

This paper focuses primarily on the following issues regarding China's data security legislation. First, the inconsistency in the denomination and definition of data and information among different countries, as well as the lack of distinction between data and information in legislation, has led to theoretical disputes. This paper analyses and discusses the

---

[2] Open Government Data Act (Open, Public, Electronic, and Necessary Government Data Act, Public Law) 2019. This Act requires public government data assets to be published as machine-readable data. The General Services Administration must maintain an online federal data catalogue to provide a single point of entry for the public to access agency data.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[4] The strategy for data focuses on putting people first in developing technology, and defending and promoting European values and rights in the digital world. Two critical pieces of legislation have been put in place to protect the rights and interests of citizens while simultaneously fostering industrial and technological development. One is The Data Governance Act (DGA) , the other is The Data Act entered into force on 11 January 2024. See 'A European Strategy for Data' (*Shaping Europe's digital future*)' (European Commission) <https://digital-strategy.ec.europa.eu/en/policies/strategy-data> accessed 20 Feb 2024.

fundamental concepts and classifications of data, legislative provisions, and the unresolved issues that need to be addressed. Second, the legitimacy of state intervention in data governance depends on adherence to the rule of law principle in exercising power. Given the extraterritorial impact of data legislation, it is essential to regulate government data collecting behaviour clearly, respect and protect enterprise data property rights, and safeguard citizens' personal data security. Thirdly, in the era of digital globalisation, cross-border data flow has become a crucial link connecting the global economy. China's proposed 'Global Data Security Initiative' reflects its fundamental stance on promoting the free flow of data and engaging in international exchanges and cooperation in the field of data security.[5] How can this concept be reflected in domestic legislation to promote the establishment of a multilateral/bilateral international rules system for data? This discussion serves as an initial consideration of this issue. Lastly, how does China's legislative framework for data security address issues arising from the rapid development of artificial intelligence in the future?

The aim of this paper is to examine the fundamental content and significance of the DSL, highlighting its strengths and weaknesses, as well as forecasting future legislative directions. This will provide a better understanding of the formulation and importance of data security legislation. This paper contains three parts. The first part introduces the basic framework of DSL. The second part discusses the existing problems with the law, and their possible solutions. The third part analyses the challenges facing future data security legislation, and anticipates to the key areas and legislative trends.

II. THE BASIC FRAMEWORK OF THE DSL

A. Legal Nature

According to the explanations to the draft DSL,[6] the DSL is regarded as

---

[5] huaxia, 'Full text: Global Initiative on Data Security' (XinhuaNet, 8 September 2020) <http://www.xinhuanet.com/english/2020-09/08/c_139352274.htm> accessed 15 Oct 2020 ; Chaeri Park, 'Knowledge Base: China's "Global Data Security Initiative"' (*全球數據安全倡議*)(*Stanford Cyber Policy Center*, 31 March 2022)<https://digichina.stanford.edu/work/knowledge-base-chinas-global-data-security-initiative/> accessed 10 Mar 2024.

[6] Liu Junchen, 'Explanation of the Draft Law on Data Security of the People's Republic of China' (China National Network , 28 June 2020), <http://www.npc.gov.cn/npc/c2/c30834/202106/t20210611_311948.html> accessed 10 Sep 2021 (劉俊臣： 《關於《中華人民共和國數據安全法（草案）》的說明》, 載中國人大網 , http://www.npc.gov.cn/npc/c2/c30834/202106/t20210611_311948.html, 2021 年 9 月 10 日訪問).

the basic law in the field of data, establishing the basic system of data security protection and management, and solving the main problems in the field of data security.[7] Its legal nature has the following characteristics:

First, the law is a security law. The law uses public power to intervene in data security protection, builds a comprehensive and systematic institutional framework for data security protection and management, uses strategies, systems and measures to build the country's ability to prevent, control and eliminate data security threats and risks, establishes the legitimacy of state behavior, and improves the country's overall data security capability.[8] There is a correlation between the DSL and the National Security Law, which is the basic positioning of the law on data security protection. The DSL is a law that takes the overall national security concept as its basic value orientation and legislative guiding ideology. In terms of the relationship between data security and national security, the National Security Law has already stipulated the principles of data security. The revised National Security Law of 2015 emphasises at a macro level that national security work should balance 'traditional security' and 'non-traditional security'. In addition to focusing on traditional security such as 'politics, homeland, and military', equal attention should be given to 'non-traditional security' such as 'economy, culture, society, technology, information, ecology, resources, and nuclear security'.[9] The National Security Law explicitly identifies the safeguarding of network and information security as a specific tenet of national security, emphasising the need to achieve secure and controllable use of core technologies, key infrastructure, and important information systems

---

[7] Article 1 of the DSL (Draft) stipulates: 'This Law is formulated in order to ensure data security, promote data exploitation and utilisation, protect the legitimate rights and interests of citizens and organisations, and safeguard national sovereignty, security and development interests.'

[8] The basic position of the law is a special law of the National Security Law and a special law for data security. In terms of specific content and system design, it mainly focuses on national security and public security. Therefore, personal data security and information protection are separately stipulated in the Personal Information Protection Law.

[9] See Article 8 of the National Security Law (Order No. 29 of the President, Standing Committee of the National People's Congress). As Xi Jinping Overall Safety Concept claims, 'We attach great importance to both traditional and non-traditional security, and build a national security system that integrates political security, homeland security, military security, economic security, cultural security, social security, technological security, information security, ecological security, resource security, and nuclear security; We attach great importance to both development and security issues. Development is the foundation of security, and security is the condition for development.' See Shi Wei, 'The First meeting of the Central National Security Commission was Held, Xi Jiping Delivers an Important Speech', (Xinhua News Agency , 15 April 2014) <http://www.gov.cn/xinwen/2014-04/15/content_2659641.htm> accessed 22 Nov 2021 (史瑋：《中央國家安全委員會第一次會議召開 習近平發表重要講話》, 載新華社 , http://www.gov.cn/xinwen/2014-04/15/content_2659641.htm，2021 年 11 月 22 日訪問).

and data in cyberspace.[10]

Second, the law is a fundamental data law. The function of basic legislation is not to solve a problem, but to provide specific guidance for the solution of the problem that depends on the matching of laws and regulations.[11] This also determines the existence of a large number of principled and sworn clauses in the language of the law.

Third, the law is an empowering law.[12] The law is a data security management law, which establishes a data security management agency and its functions and responsibilities, and stipulates the obligations of data activity subjects in data security. In terms of data security management, it should be fully coordinated with the Cybersecurity Law of the PRC[13] to avoid the waste of legislative resources, regulatory duplication and vacuum, and the burden on the data industry caused by the cross-over and duplication of system design.

B. Applicable Objects and Scope

The applicable objects of the DSL include three levels. One is data, which refers to any electronic or other records of information. The DSL has modified the data definition in the draft by removing the phrase 'other electronic forms' and replacing it with 'other means', which broadens the scope of data covered. The second is data security, which refers to the ability to ensure effective protection and legal use of data and maintain a secure state by taking necessary measures. The third is data processing, including data collection, storage, use, processing, transmission, provision and disclosure, etc. It is consistent with the provisions of the Civil Code

[10] Article 25 of the National Security Law stipulates that the state shall build a network and information security guarantee system, improve network and information security protection capability, strengthen the innovation research, development, and application of network and information technologies, realise the controllable security of the core technologies and crucial infrastructure of network and information and the information systems and data in important fields.

[11] Huang Daoli, Yuan Hao, Hu Wenhua, 'Legislative Background, Legislative Positioning and System Design of the Draft DSL' (2020) 8 Information Security and Communication privacy 9 (黃道麗、原浩、胡文華：《數據安全法 (草案)》的立法背景、立法定位與制度設計，載《信息安全與通信保密》2020 年第 8 期，第 9 頁) .

[12] The Law mainly stipulates the regulatory system for data security, establishes a management system for data security through data classification, and grants regulatory agencies the authority to supervise data security.

[13] For example, Article 21 of Cybersecurity Law stipulates: 'The state shall implement the rules for graded protection of cybersecurity.' Article 21 (4) stipulates: 'Taking measures such as data categorisation, and back-up and encryption of key law.' Article 22 stipulates: '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.' All of these provisions establish powers and obligations for network administrators and operators that are similar to those outlined in data security laws, which can lead to conflicts in practical operation.

on personal information processing (collection, storage, use, processing, transmission, provision and disclosure, etc.).[14]

The DSL's territorial scope clearly indicates the extraterritorial regulatory effect, emphasising that data processing activities conducted outside China that harm China's national security, public interests, or the lawful rights and interests of citizens and organisations will be subject to this law. This rule is a fundamental expression of the data sovereignty concept in legal provisions.[15] In fact, China's previous legislation has already explored the extraterritorial effect of legal application, such as the provisions on foreign monopoly behavior under the Anti-Monopoly Law and the legal responsibility of foreign entities for endangering domestic critical information infrastructure under the Cybersecurity Law.[16]

C. Amendments and Changes

Compared with the Drafts of the previous two deliberations, the current DSL has the following major amendments and changes in important systems:

1. The Establishment of a Work Coordination Mechanism

Data security involves various industries and fields, as well as the responsibilities of multiple departments. The Draft stipulates the decision-making and overall coordination responsibilities of the central national security leadership institution for data security work,

[14] Article 1035 of Civil Code, Section 2 (Order No. 45 of the President of the People's Republic of China, National People's Congress), 'The processing of personal information includes the collection, storage, use, processing, transmission, provision and disclosure, and the like, of the personal information.'

[15] With the development of the internet economy, various cross-border internet service providers have extended their services to every corner of the world. While some internet service providers still have a considerable user base within a certain geographical area, such as Line in Japan and Yandex in Russia, social networking platforms Facebook and Twitter have become the preferred choice for most residents of most countries to stay informed. TikTok, launched by China in recent years, has also attracted a large number of users overseas. The cross-border flow of data and the extraterritorial effect of data regulation are the inevitable result and requirement of the development of the data economy. See Xiong Jiani, 'Study on the Sufficient Protection Principle in Cross-Border Flow of Personal Data in the EU and Its Enlightenment to China' [2020] Master's e-journal 3 (熊佳妮：《歐盟個人數據跨境流動中"充分性保護原則"的研究及對我國的啟示》，廣東外語外貿大學 2020 年碩士畢業論文，第 3 頁); Luo Qianyi, 'On the Legal Application of Cross-Border Infringement Disputes of Personal Data Rights' [2020] Master's e-journal 8 (羅芊怡：《論個人數據權跨境侵權糾紛的法律適用問題》，外交學院 2020 年畢業論文，第 8 頁).

[16] See Article 2 of the Anti-Monopoly Law (Order of the President of the People's Republic of China No.68, Standing Committee of the National People's Congress 30 Augest 2007): 'This Law applies to monopolistic conducts in economic activities within the territory of the People's Republic of China; this Law applies to monopolistic conducts outside the territory of the People's Republic of China that have the effect of eliminating or restricting competition in domestic markets.' Article 75 of the Cybersecurity Law (Order No. 53 of the President, Standing Committee of the National People's Congress 11-07-2016): 'Where any overseas institution, organisation or individual attacks, intrudes into, disturbs, destroys or otherwise damages the critical information infrastructure of the People's Republic of China, causing any serious consequences, the violator shall be subject to legal liability according to law; and the public security department and relevant departments under the State Council may decide to freeze the property of or take any other necessary sanctions against such institution, organisation or individual.'

strengthening the organisation and leadership of data security work. At the same time, the responsibilities of relevant industry departments and regulatory authorities for data security supervision are specified, but the authority and coordination between different levels and departments are not clearly defined.[17] It adds provisions to establish a national data security coordination mechanism. Among them, the leading central national security agency is to be the leading organ for data security, and its responsibilities are to include decision-making and coordination of the national data security work.[18] All localities and departments are to bear responsibility for the management of the data collected or generated in their work as well as for the data security thereof.

2. Clear Categorisation and Classification and key law System

Data categorisation and classification protection is to protect data according to the type and level to meet the protection requirements of different data. The DSL clarifies the data as 'core data' which implements a stricter management system related to national security, the lifeline of the national economy, important to people's livelihoods, and to major public interests. It will implement stricter control over key and highly sensitive data. The DSL establishes categorised and classified standards for data based on the importance of data in economic and social development.[19] On the basis of the standards, the key law protection directory is determined, and protection of the data listed in the directory is emphasised. The 'DSL' carries on the Cybersecurity law hierarchical handling of network security incidents and network security grade protection system 2.0 national standards, and also refers to the existing securities and futures industry data, and other classification systems. Relevant state departments shall formulate relevant standards, and support enterprises and social

---

[17] Article 6 of the DSL (draft) stipulates, 'The national cyberspace affairs department shall be in charge of the overall planning and coordination of network data security and the related supervision and regulation in accordance with the provisions of this Law and other relevant laws and administrative regulations.'

[18] Article 5 of the DSL stipulates that the central leading authority for national security shall be responsible for the decision-making, deliberation and coordination of the national data security work; researching, formulating, and guiding the implementation of the national data security strategy and related major guidelines and policies; coordinating major matters and important work in respect of national data security; and establishing a coordination mechanism for national data security.

[19] Article 21 (1) of the DSL (Order No. 84 of the President of the People's Republic of China, Standing Committee of the National People's Congress): 'The state shall establish a categorised and classified system and carry out data protection based on the importance of the data in economic and social development, as well as the extent of harm to national security, public interests, or the lawful rights and interests of individuals or organisations that will be caused once the data are altered, destroyed, leaked, or illegally obtained or used. The coordination mechanism for national data security shall coordinate the relevant departments to formulate a catalogue of key laws and strengthen protection of key laws.'

organisations to participate in the formulation of standards.[20]

3. The Protection of the Intelligent Rights for the Elderly and the Disabled

With the wide application of intelligent services, the problem of the 'digital divide' faced by vulnerable groups in society has become increasingly prominent. In order to promote further the solution of the difficulties encountered by the elderly in the use of intelligent technology, so that they can better share the results of information development, the General Office of the State Council issued the Notice on the Implementation Plan to solve Effectively the difficulties of the Elderly in the use of intelligent technology, but has not paid attention to the difficulties of the application of intelligent technology for the disabled.[21] The DSL, for the first time in the form of legislation, confirms and guarantees the rights of the elderly and the disabled in terms of intelligent services and applications.[22] The elderly and persons with disabilities shall enjoy the right to convenience in using intelligent applications and services in the fields of government services, medical and health care, transportation, education, etc. Relevant institutions and enterprises shall fully consider the needs of the elderly and persons with disabilities and avoid causing obstacles to their daily lives. This is one of the highlights and features of the DSL.

4. The Improvement of the Security and Openness of Government Data

The openness and sharing of government data will affect the national economy and people's livelihoods in many industries such as healthcare, education and transportation. In order to ensure the security of government data and promote the open utilisation of government data, the fifth chapter of the DSL is dedicated to making clear provisions on the security and openness of government data and enhancing the security mechanism in opening and sharing of government data. The

---

[20] Article 17 of the DSL stipulates: 'The state shall advance the forming of the standards for data development and the standards for data utilisation technologies and data security. The department in charge of standardisation under the State Council and other relevant departments under the State Council shall, within the scopes of their respective duties and functions, organise the establishment of, and make revisions in due time to the standards for, technologies and products for data development and data utilisation and the standards for data security. The state shall support enterprises, social groups, and education or research institutions, etc. in their participation in the establishment of such standards.'

[21] 'The General Office of the State Council issued a Notice on the Implementation Plan to solve effectively the difficulties in the use of intelligent Technology for the elderly' (China Government website, 24 Novermber 2020)<http://www.gov.cn/zhengce/content/2020-11/24/content_5563804.htm> accessed 2 Oct 2021 (《國務院辦公廳關於切實解決老年人運用智能技術困難實施方案的通知》，載中國政府網，http://www.gov.cn/zhengce/content/2020-11/24/content_5563804.htm，2021 年 10 月 2 日訪問).

[22] Article 15 of the DSL stipulates: 'The state supports development and utilisation of data to render public services smarter. In providing smarter public services, the needs of the elderly and the disabled shall be taken into full account to avoid posing obstacles to their daily lives.'

DSL establishes the government data security and open system from four aspects. First, it commits to continuing to promote the construction of e-government at all levels of government in general, and to improve the ability to use data to serve economic and social development.[23] Second, it commits to clear use of the procedures for collecting data. State organs shall use the collected data within the scope of their statutory duties in accordance with the conditions and procedures prescribed by laws and administrative regulations, and shall not disclose or illegally provide others with personal information, trade secrets and confidential business information that they have come to know in the course of performing their duties.[24] Governments at all levels are required to establish data security protection systems and implement data security protection responsibilities. Third, it commits to clarify the procedures for entrusting third parties to collect data. Provisions shall be made on the examination and approval requirements and supervision obligations of state organs in entrusting others to store, process or provide government data to others.[25] Fourth, it commits to developing an open catalogue. State organs are required to disclose government data in a timely and accurate manner in accordance with regulations, formulate an open catalogue of government data, build an open platform for government data, and promote the open use of government data.[26]

5. The Enhancement of Penalties for Violations

The locus of legal responsibility in the Draft is not clear, which quickly became the main concern of the public in relation to DSL. The DSL has

[23] Article 37 of the DSL stipulates: 'The state shall make great efforts to promote the development of e-government, make government databases more scientific, accurate, and time-efficient, and improve the ability of using data to serve economic and social development.'

[24] Article 38 of the DSL stipulates: 'Where state organs need to collect or use data to perform their statutory duties, they shall collect or use data within the scope as needed for performance of their statutory duties and under the conditions and procedures provided by laws and administrative regulations. They shall, in accordance with the law, preserve the confidentiality of the data accessed in the course of performing their duties, such as personal privacy, personal information, trade secrets, and confidential business information, and shall not divulge such data or illegally provide them to others.'

[25] Article 40 of the DSL stipulates: 'Where a state organ entrusts others to construct or maintain e-government systems, or to store or process government data, the state organ shall go through strict approval procedures, and shall supervise the entrusted party in the performance of data security protection obligations. The entrusted party shall perform its data security protection obligations in accordance with the provisions of laws, regulations, and contracts signed, and shall not retain, use, divulge, or provide others with government data without authorisation.'

[26] Article 41 of the DSL stipulates that 'State organs shall, under the principles of fairness, equality and convenience for the people, disclose government data in a timely and accurate manner in accordance with the provisions, except those which shall not be disclosed in accordance with the law.' Article 42 states: 'The state shall formulate the catalogue of open government data, build an open, uniform, standardised, interconnected, safe and controllable government data platform, and promote the release and utilisation of government data.'

improved on this issue, and the enforceability of the law mainly relies on legitimate sources of data, data classification and data responsibility.[27] In terms of legal sources of data, the law requires the data provider to explain the data source, review the identities of both parties to the transaction, and retain audit and transaction records to form a complete data flow chain, in which it is easy to clarify responsibility and traceability. In terms of data responsibility, regulatory agencies in various industries have assumed supervision responsibilities, increased supervision efforts, clarified the exercise conditions and punishment objects of ordered rectifications, warnings and fines, and increased the amount of the penalties. In terms of data classification, key law processors should clarify the data security responsible person and management body, fulfil their data security protection responsibilities, carry out risk monitoring and submit risk assessment reports.

III. PROBLEMS AND SUGGESTIONS

A. Value and Positioning: The Legislative Dilemma of Balancing Security and Development

The overall national security concept emphasises 'attaching importance to both development issues and security issues'.[28] It is required that the value and positioning of the DSL should satisfy both 'security and development'. How to reflect the coordination and unity of the values of security and development in the DSL, especially in the construction of specific systems to implement the basic spirit of the overall national security concept, detailed system support, and policy discourse on legal norms are the basic issues of which lawmakers need to balance proper consideration.

The first article of the DSL states that the legislative purposes of the DSL are four. First, to ensure data security; second, to promote the development and utilisation of data; third, to protect the legitimate rights and interests of citizens and organisations; and fourth, to safeguard national sovereignty, security and development interests.[29] From the

---

[27] Tencent data security expert Liu Haiyang said in an interview with a reporter from China Electronics News that the release of the DSL needs to focus on three keywords: data responsibility, legal sources of data, and classification. See Song Jing, 'What Important Information Does the Newly Released DSL Reveal?', (China Electronics News,12 June 2021) <http://m.cena.com.cn/data/20210612/112134.html> accessed 14 Sep 2021 (宋婧：《剛剛出爐的《數據安全法》透露了哪些重要信息？》，載《中國電子報》，https://m.cena.com.cn/data/20210612/112134.html，2021 年 9 月 14 日訪問).

[28] Shi (n 9).

[29] Article 1 of the DSL (Draft).

point of view of the system design of the DSL, including these multiple legislative objectives in one law may not only produce conflicts in value, but also bring difficulties to law enforcement. The second chapter of the DSL is 'Data security and development', but all the chapters are declarative and principled provisions, without specific institutional arrangements, and need to be clarified by other relevant laws and regulations. Only three deal with the data transaction management systems, and Article 19 affirms the legal status of data transaction activities for the first time;[30] Article 33 stipulates the obligations of data transaction intermediary service agencies;[31] Article 47 provides for the legal responsibility of data trading intermediaries to fulfill their obligations.[32] The DSL does not cover the basic rules on data rights, data circulation, and protection of personal information, which must be clarified through the Personal Information Protection Act and relevant data legislation.

As for the legislative positioning and legislative purpose of the DSL, the discussion of the draft in academic circles is still controversial. It is argued that the theoretical endeavours to define the essence of data in private law are subject to certain limitations, and there are structural difficulties in incorporating data into the rights system of private law. Data legislation is a system of public rules between data sharing and control.[33] Conversely, the opposing view holds that the rationality of the intervention of private law in data security law can be demonstrated from the international background. It is held that the positioning of the DSL has undergone three transitions: namely, the transition from a special law of the National Security Law to a fundamental law of the Data Security Law, the transition from a sole legislative objective of national security to

[30] Article 19 of the DSL stipulates that the state shall establish sound systems for data trading management, standardise data trading activities, and foster a data trading market.

[31] Article 33 of the DSL stipulates: 'When providing services, data transaction intermediaries shall require data providers to specify the sources of the data, verify the identities of both parties to the transactions, and retain the verification and transaction records.'

[32] Article 47 of the DSL stipulates that where a data transaction intermediary fails to perform the obligations prescribed in Article 33 of this Law, it shall be ordered by the competent department to make rectifications; its illegal gains, if any, shall be confiscated, and it shall also be fined not less than the amount of, but not more than ten times the amount of the illegal gains; if there are no illegal gains or the illegal gains are less than RMB 100,000 yuan, it shall be fined not less than RMB 100,000 yuan but not more than RMB 1 million yuan. It may be concurrently ordered to suspend the relevant business or suspend operations for rectification, or have relevant business permits or the business license revoked. The directly liable persons in charge and other directly liable persons shall be fined not less than RMB 10,000 yuan but not more than RMB 100,000 yuan.

[33] See Mei Xiaying, 'Limitations of Private law and construction of Public order in data protection between Sharing and control '(2019) 31(4) Peking University Law Journal 845–870 (梅夏英： 《在分享和控制之間 數據保護的私法局限和公共秩序構建》，載《中外法學》2019 第 4 期，第 845–870 頁).

a compound one, and the transition of the legislative status from public law to a mixture of public and private law. The DSL should be a law where power and rights are balanced and coexist.[34] Ke Xu also makes the point that the ultimate goal of data security legislation is development.[35] Although this view once dominated the formulation of some data security policies, in later policy documents, policymakers have rejected the public-private mixed regulation path.[36] Further, one can take into account the relationship between data security and the digital economy, the legislative goal of the DSL is to put security governance on an equal footing with the development of informatisation and establish it as a guarantee for the development of the digital economy.[37] The DSL should be improved in terms of the relationship between data security governance and the basis of private law, should establish a data property rights system, and should transform data resource achievements through public-private collaboration.[38] It is argued that the Draft faces problems of unclear legislative positioning and of pursuing too many goals, and that the diversified legislative goals are difficult to achieve simultaneously in data security legislation. Contrary to the mainstream view, Xuzhi Han argued that although the DSL is the first single piece of legislation in China's data field, it is difficult for it to act as a basic law in the data field, and it should return to the basic position of safeguarding national security.[39] The legislative purpose of the DSL should be to 'safeguard national security,

---

[34] See Xu Ke, 'Establish and improve the legal system for data security' *Economic Information Daily* (Beijing, 15 September 2020) <http://dz.jjckb.cn/www/pages/webpage2009/html/2020-09/15/node_9.htm> accessed 16 Oct 2020 (許可: 《建立完善數據安全法律體系》載《經濟參考報》, http://dz.jjckb.cn/www/pages/webpage2009/html/2020-09/15/node_9.htm, 2020 年 10 月 16 日訪問).

[35] See Xu Ke ,'Data Security Law: Positioning, Position and Institutional Structure' (2019) 3 Economic and trade law review 52–60 (許可: 《數據安全法 : 定位、立場與制度構造》, 載《經貿法律評論》2019 年第 3 期, 第 52–60 頁).

[36] The 'Measures for the Security Assessment of Personal Information Export (Draft for Comment)' issued by the Cyberspace Administration of China has abandoned the idea of combining the regulation of the export of key law and personal information. This indicates that the relevant departments have realised the harm brought about by the mixture of public and private regulations.

[37] See Long Weiqiu, 'Safe and Reliable Rule of Law and New Regulatory Requirements in the Digital Age' (2021) 18 Media 19–21 (龍衛球: 《數字化時代安全可信的法治保障與新型監管要求》, 載《傳媒》2021 年第 18 期, 第 19–21 頁).

[38] See Long Weiqiu, 'Establish and improve the legal system for data security' *Economic Information Daily* (Beijing, 15 September 2020), <http://www.jjckb.cn/2020-09/15/c_139368867.htm> accessed 21 Dec 2024 (龍衛球: 《建立完善數據安全法律體系》, 載《經濟參考報》, http://www.jjckb.cn/2020-09/15/c_139368867.htm, 2024 年 12 月 21 日訪問).

[39] See Han Xuzhi, 'Positioning and Direction of China's Data Security Legislation - Suggestions for Amendments to the Draft DSL' (2020) 39 (5) Journal of Xihua University (Philosophy and Social Sciences Edition) 27–28 (鄭鈜、汪灝、劉明等: 《數據安全立法的機理、表達與規範——"數據安全法治暨〈數據安全法〉立法研討會"發言摘錄》, 載《西華大學學報 (哲學社會科學版)》2020 年第 5 期, 第 27–28 頁).

data sovereignty and social public interests, and promote the healthy development of the data economy and data open sharing mechanism', rather than to protect the data-related property interests enjoyed by specific private entities.[40] The final DSL does not address these contentious issues. So far, law enforcement based on the DSL has been relatively rare compared with those undertaken in relation to the Personal Information Protection Law and the Cyber Security Law. This is closely related to the lag in the implementation of the DSL and the many discussions and even disputes surrounding the positioning of the DSL at the beginning of its implementation.[41]

B. Re-exploration of the Basic Categories of Data

From the perspective of the relevant legislation of various countries, the appellation and definition of data and information in various countries are not uniform, and most countries do not distinguish between data and information in legislation, and this has caused a lot of disputes in theory. According to the International Organisation for Standardisation, 'Data and information should be said to be one and the same. Data is the form and carrier of information, and information is the content that data can express.'[42] This announcement does not clarify the definition at all but in fact makes it more confused. Information is a central concept in data protection law under the General Data Protection Regulation (GDPR). Yet, there is no clear definition of information in this example of European data protection law or in prior European Union (EU) data protection law, nor is a structured and comprehensive definition provided in the relevant jurisprudence.[43] It terms of both legislative and practical issues there is risk or danger when personal data is defined too widely

---

[40] See Zhu Xuezhong , Dai Zhizai, 'The Value and System Positioning of the DSL from the Perspective of Overall National Security' (2020) 8 E-Government 82–92 (朱雪忠、代志在：《總體國家安全觀視域下 < 數據安全法 > 的價值與體系定位》，載《電子政務》2020 年第 8 期，第 82–92 頁). The legislative purpose of DSL is still debated in academic circles. Some scholars believe that 'the DSL' mainly protects enterprise data from intrusion, theft, destruction and illegal use by others. It deals mainly with the relationship between enterprises and other enterprises and individuals, and mainly protects the legitimate commercial interests of enterprises in data.

[41] See Hong Yanqing, 'The systematic logic and implementation optimization of China's Data Security Law ' (2023) 2 Law Science Magazine 38–39 (洪延青：《我國數據安全法的體系邏輯與實施優化》，載《法學雜志》2023 年第 2 期，第 38–39 頁).

[42] ISO/IEC 27040:2015. See Clare Naden, 'Keeping Data Safe—What's Your Back Up?' (Information Technology, 13 January 2015) <https://www.iso.org/news/2015/01/Ref1926.html> accessed 20 May 2024.

[43] See Dara Hallinan, Raphal Gellert, 'The Concept of "Information": An Invisible Problem in the GDPR' (2020) 17 (2) Scripted 269–71.

or narrowly.[44] The principal limit to the concept of personal data is that information must 'relate to' an individual for that information to be that individual's personal data. It is, however, not clear when information 'relates to' an individual under existing data protection legislation. The courts in the UK and the EU have sought to address this problem in the case law, but the approaches adopted by the courts have not been wholly consistent or satisfactory.[45] In the context of US literature, legal academic and policy discourse generally presumes that information privacy and data security are interchangeable goals. However, this view is an oversimplification of the relationship between the two fields. As Lauren Henry contends, data security has separate objectives from information privacy that are agnostic or even in opposition to information privacy.[46] Raphaël Gellert argues that in the legal definition of personal data, data is information. This is in line both with a literal reading of the GDPR definition (art. 4.1 GDPR) and with the present overview of information theory, and the inability of data protection law meaningfully to regulate machine learning algorithms. Therefore, the exploration of the different meanings of data and information at stake in data protection law and in machine learning, and their different yet interrelated meanings, point to the need for a set of new regulatory principles.[47]

The definition of data in academic and legal circles in China has been uncertain since the preparation of the DSL. There is a dearth of specialised

---

[44] See Stephen Allison, 'The Concept of Personal Data under the Data Protection Regime' (2009) 1 Edinburgh Student L. REV, 48. 'While some tensions exist between these different policy aspirations, it would appear that a purposive view of the PDPA would mean according a broad and expansive reading to personal data especially given the general scheme of the Act', Warren B. Chik & Pang Keep Ying Joey, 'The Meaning and Scope of Personal Data under the Singapore Personal Data Protection Act' (2014) 26 SAcLJ 354–94, at 394. See also Nadezhda Purtova, 'The law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 (1) Law, Innovation And Technology 40–81.

[45] See Benjamin Wong, 'Delimiting the Concept of Personal Data after the GDPR' (2019) 39 Legal Studies, 517.

[46] See Lauren Henry, 'Information Privacy and Data Security' (2015) 2015 Cardozo L Rev De-Novo 107–9. The author proposes a definition of information privacy as combining the two: that is those policies with respect to collected personal information that reflect an individual's liberty interest in deciding what to do with that information, and social norms regarding how personal information should be used, distributed, and processed. The definition of data security understanding is similar in the law literature, the case law, and in industry: it roughly means institutional rules and technical methods that an institution uses to ensure that data is only accessed by authorised persons.

[47] Raphaël Gellert, 'Comparing definitions of data and information in data protection law and machine learning: A useful way forward to meaningfully regulate algorithms?' (2022) 16 Regulation & Governance 156–72.

research regarding the relationship between data and information.[48] Disputes among Chinese scholars as to which appellation can better reflect the legislative purpose and comprehensively cover its connotations and extensions have existed. However, the current dominant view of the academic community tends to use the title of personal information, which can be supported by the fact of the passage and implementation of Personal Information Protection Law. One side believes that data is a digital record of facts and activities, and that information is what data expresses, but the other criticizes as highly questionable the view of 'data' as the form or carrier of 'information' and the assertion that 'information' and 'data' stand in the relationship of content to form or carrier.[49] People are more concerned about the value brought by the information, rather than the data itself, so the enactment of laws is more inclined to protect the connotation of personal data, namely personal information, rather than being limited to the objective data.[50] As a matter of fact, this is not true concerning the Hong Kong and Macao version of Data Security Law.[51]

The Cybersecurity Law does not define 'data', but adopts a definition

---

[48] See Mei Xiaying,'The legal Attribute of Data and its Orientation in Civil Law' (2016) 9 Social Sciences in China, 164–184 (梅夏英: 《數據的法律屬性及其民法定位》, 載《中國社會科學》2016 年第 9 期, 第 164–184 頁); Ji Hailong , 'Positioning and Protection of Data in Private Law' (2018) 41(6) Law Research 72–91 (紀海龍: 《數據的私法定位與保護》, 載《法學研究》2018 年第 6 期, 第 72–91 頁); Li Guyuan, 'Public Data Governance from the Perspective of Data Security Law (Draft)' (2020) 8 Information Security and Communications Privacy 29–30 (李顧元: 《< 數據安全法 (草案)> 視野下的公共數據治理》, 載《信息安全與通信保密》2020 年第 8 期, 第 29–30 頁); Zhi Zhenfeng, 'Chinese Approach to Data Security Legislation' (2020) 8 Information Security and Communications Privacy 2–4 (支振鋒: 《貢獻數據安全立法的中國方案》, 載《信息安全與通訊保密》2020 年第 8 期, 第 2–4 頁).

[49] Data is a record of things, states, etc. The content carried by data includes information and non-information. The carrier of information can also be the carrier of data, in the form of bits, graphics or other symbols. See Li Aijun , 'Attributes of Data Rights and Legal Characteristics' (2018) 3 Eastern Law 64–74 (李愛君: 《數據權利屬性與法律特徵》, 載《東方法學》2018 年第 3 期, 第 64–74 頁). See also Tan Li, 'The Definition of Information and Data and Its Legal Analysis' (2022) 325 (07) Social Science Front 224–227 (譚立: 《信息、數據的界定與法律分析》, 載《社會科學戰線》2022 年第 7 期, 第 224–227). He argued that the definition of data in DSL should take into account the needs of applications in various disciplines and fields. However, this law regards all recorded materials about objective facts as exceeding the realistic basis, as difficult to achieve in practice and prone to generating chaotic data.

[50] In English, " 數據 " and " 資料 " are both data, so there is no essential difference between personal " 數據 " and personal " 資料 ".

[51] In December 1996, Hong Kong implemented the Personal Data (Privacy) Ordinance, which is one of the first comprehensive pieces of legislation to protect personal data privacy in Asia. Macao enacted the Personal Data Protection Law in 2005, which borrowed and absorbed from the principles and contents of the European Union's General Data Protection Regulation (GDPR). Both bills aim to regulate substantive content and form, whose effects cannot be diminished due to the titles or names.

of 'network data'[52] and clarifies the 'personal information' simultaneously.[53] The CyberSecurity Law stipulates that personal information includes information recorded electronically and in other ways. The electronic data is called 'network data'. It is mentioned in the literature that before the concept of network security emerged, information security was generally used. Information is only one aspect of cyberspace, and now the term network data security is more commonly used.[54] In addition, in the cybersecurity law, network security in a broad sense encompasses data security and personal information security. The distinction between data security and network security is not clear from the legal perspective.[55] However, the Cybersecurity Law does not define non-electronic information (information recorded in other ways) other than personal information. Article 127 of the General Provisions of the Civil Law states: 'Where there are provisions of the law on the protection of data and network virtual property, such provisions shall prevail'. The newly promulgated 'Civil Code' follows this expression, juxtaposing 'data' with 'network virtual property', and the connotation of data is more inclined to electronic information.[56] One breakthrough in the DSL draft is the definition of data. Article 3 of the law states that 'for the purposes of this Law, data means any record of information in electronic or non-electronic form'. That is, in addition to the 'network data' defined in the 'Cybersecurity Law', the 'non-electronic form of information recording' is

---

[52] See Article 76 (4) of the Cybersecurity Law: 'network data' refers to all kinds of electronic data collected, stored, transmitted, processed and generated through the network.

[53] Article 76 (5) of the Cybersecurity Law: 'Personal information' refers to all kinds of information recorded in an electronic or other forms, which can be used independently or in combination with other information, to identify a natural person's identity, including but not limited to the natural person's name, date of birth, identity certificate number, personal biometric information, address, telephone number, etc.'

[54] See Zhang Yan, 'The Dual Basis of Legislation on Cybersecurity ' (2021) 310 (10) Social Sciences in China 83–87 (張曩: 《網絡空間安全立法的雙重基礎》, 載《中國社會科學》2021 年第 10 期, 第 83–87 頁).

[55] See Ying Song, 'The Deficiencies and Improvements of National Security Legislation in China ' (2021) 5 Gansu Social Sciences 136–138 (宋穎: 《我國國家安全立法的不足與完善》, 載《甘肅社會科學》2021 年第 5 期, 第 136–138 頁).

[56] Article 111 of Chapter 5 of the Civil Code provides that, 'The personal information of natural persons is protected by law. Any organisation or individual that needs to access other's personal information must do so in accordance with the law, and guarantee the safety of such information, and may not illegally collect, use, process or transmit the other's personal information, or illegally trade, provide or publicise such information.' Chapter VI of the Civil Code provides for the right to privacy and the protection of personal information. Article 1034 states: 'The personal information of natural persons is protected by law. Personal information is information recorded electronically or otherwise that can be used by itself or in combination with other information, to identify a natural person, including the name, date of birth, identification number, biometric information, resident address, telephone number, e-mail address, health information, whereabouts, and the like, of the person.'

also included in the category of data. According to this definition, paper archival information and other written records of information are also data. An outstanding feature of the Archives Law (2020 Amendment) is that special provisions are made for the protection of electronic archives.[57] The Archives Law (2020 Amendment) reflects the trend of information digitisation to a certain extent, and adopts the same legislative extension for 'information' and 'data'.[58] Although the Archives Law (2020 Amendment) improved the concept of 'archives' and clearly defined the legal effect and evidential value of electronic archives in the newly added chapter of 'Archives Informatisation Construction', it did not adequately detail the legal concept of 'electronic archives'.[59] The final DSL defines data as 'any record of information, electronic or otherwise'. It adopted the definition of data in the Cybersecurity Law but abandoned the expression in the Draft.

The DSL adopts a broad definition of 'data', while the Cybersecurity Law adopts a broad definition of 'information'. Is data then identical to information, and can the two be applied interchangeably in different scenarios? If so, why do different terms for the same normative object lead to conceptual confusion and theoretical disputes?[60] It is worth noting that the confusion and ambiguity of data and information can easily lead

---

[57] Article 35 of the Archives Law (revised in 2020) (Order No. 47 of the President of the People's Republic of China, Standing Committee of the National People's Congress 20 June 2020): 'People's governments at all levels shall incorporate archival informatisation into their informatisation development plans, and ensure the safe preservation and effective use of archival digital resources such as electronic archives and digital achievements of traditional carrier archives."

[58] The digitalisation form refers to the electronic form with digital codes such as 0 and 1 as the underlying structure to present the attributes and related situations of people, things and events. It can be seen that digitalisation is electronicisation. All information material presented in this form belong to data (that is, electronic data). See Tan, (n 49) 224–226.

[59] 'Electronic archives' have intersections with 'data' in terms of substantive attributes, existence forms and management models. Electronic archives security and data security overlap in terms of the objects, links and contents of governance. Therefore, the definition of 'data security' in the DSL can be used as the definition of the concept of 'electronic archives security'. See Wang Qun, Li Haoran , 'The Current Review and Improvement Path of Electronic Archive Security Legislation in China' (2024) 1 Archives Science Study 69–70 （王群、李浩然: 《我國電子檔案安全立法的現狀考察與完善路徑》, 載《檔案學研究》2024 年第 1 期, 第 69–76 頁).

[60] It is precisely because legislators mixed and misused the term 'data' when organising legal language that the 'data' in legal texts is variable and the semantic connotation is unstable, which undermines the precision of legal terms and concepts, and as a result, the extension of 'data' naturally cannot be determined. See Zhang Hong, "Data" in Chinese Legal Texts: Semantics, Norms and Genealogy' (2022) 5 Journal of Comparative Law 61–66 (張紅: 《我國法律文本中的"數據": 語義、規範及其譜系》, 載《比較法研究》2022 年第 5 期, 第 61–66 頁).

to the deviation in rights setting and judicial protection.[61] The concepts of network data, personal information and other information in other relevant legislation should be sorted out and adjusted together, so as to facilitate the conceptual convergence between different legislation.

Another core concept in the DSL is 'key data'. However, the law lacks a definition of 'key data'. Articles 21,[62] 27[63] and 30[64] all deal with the specification of key data. Although the identification mechanism of key data can be established under this system, the lack of relevant normative definition will still result in the judgment of key data lacking standards. The DSL proposes a new concept of 'core data', while the article also includes the content of key data, but does not specify the relationship between key data and core data. Many DSLs and policy documents, such as the Cybersecurity Law, Data Security Management Measures, and Exit Security Assessment Measures for Personal Information and key law, all use the concept of 'key data', but they do not point out its specific meaning, which brings ambiguity and uncertainty to the framework and implementation of the procedural system.[65]

The latest national standard for data classification and grading

[61] Data and information are often used fuzzily in judicial adjudication and academic research, and form three types of information and data, information contains data, data contains information. The danger of this kind of vagueness is that it will not only lead to the deviation in right setting, but also cause trouble for the court in protecting the information right and conducting legal argumentation. It must be made clear that information focuses on content while data focuses on form, which has different legal characteristics, is associated with different right objects, and has the possibility of dynamic transformation under certain conditions. See Han Xuzhi, 'Fuzzy Use of Information Rights and Its Consequences: Based on the analysis of Mixed Use of Information and Data' (2020) 1 Journal of East China University of Political Science and Law 85–96 (韓旭至：《信息權利範疇的模糊性使用及其後果——基於對信息、數據混用的分析》, 載《華東政法大學學報》2020 年第 1 期, 第 85–96 頁).

[62] Article 21 of the DSL stipulates: 'The state shall establish a categorised and classified system and carry out data protection based on the importance of the data in economic and social development, as well as the extent of harm to national security, public interests, or the lawful rights and interests of individuals or organisations that will be caused once the data are altered, destroyed, leaked, or illegally obtained or used. The coordination mechanism for national data security shall coordinate the relevant departments to formulate a catalogue of key law and strengthen protection of key law.'

[63] The second paragraph of Article 27 of the DSL stipulates: 'The processing of key law shall establish a data security person and management body to implement the responsibility for data security protection.'

[64] Article 30 of the DSL states: 'Processors of key data shall, in accordance with regulations, carry out regular risk assessments of their data processing activities and submit risk assessment reports to the relevant competent authorities.' Paragraph 2 provides: 'The risk assessment report shall include the type and quantity of key data processed, the situation of data processing activities carried out, the data security risks faced and measures to deal with them.'

[65] The 'key data' in the 'Guidelines for the Assessment of Outbound Security of Information Security Technical Data (Draft)' refers to the data (including original data and derived data) collected and generated by the Chinese government, enterprises and individuals in China, which does not involve state secrets, but is closely related to national security, economic development and public interests, once it is disclosed, lost, abused, tampered with or destroyed without authorisation. Or data that, after aggregation, integration, and analysis, may cause serious consequences such as endangering national security and social public interests.

issued in 2024 provided a relatively detailed set of rules to identify core data, key data and general data.[66] Given that the DSL is vague about the specific classification method of data, previously there were actually two understandings on this issue. One was that national core data is independent of key data; the other is that national core data is the more key law among the key data.[67] The definition of the core data, key data that stipulated in Rules for Data Classification and Grading verified the second point of view, that is, that the core data is the key data which may result in extremely serious harm.[68] Accordingly, the characteristics of the core data and key data include that the data reach a relatively high or certain level of accuracy, scale, depth or importance, and are directly related to specific fields, specific groups and specific regions. In addition, the Appendix to the Standard also gives the considerations for identifying key data, including 17 aspects such as military, scientific and technological strength, resources and environment, strategic new domains such as space, deep sea and polar regions, as well as biological security. However, room is still left to analyse and explore what the exact meaning of the key data and core data is, and how to apply the rules to distinguish the two in practice. At the same time, the identification mechanism, protection methods, legal responsibilities and relief channels of key data also need to be further clarified.[69] In terms of content, for the sake of national interests and national security needs, it should be straightforward to implement key protection for energy, basic industry, transportation, food, gene,

---

[66] GB/T 43697-2024 'Data Security Technology - Rules for Data Classification and Grading', is a recommended national standard issued by the National Information Security Standardisation Technical Committee on March 15, 2024. It will be implemented on October 1, 2024. For more details please see https://std.samr.gov.cn/search/std?q=.

[67] See Lan Lan, 'Key Data from the Perspective of Data Security Legislation: Connotation, Identification and Protection' (2022) 1 (02) Front of Thought and Theory 106–111 (藍藍：《數據安全立法視角下的重要數據 : 內涵、識別與保護》，載《思想理論戰線》2022 年第 2 期，第 106–111).

[68] See Xu Qi, Hu Xiaoyan, Zou Ziming, Tong Jizhou, 'Research on the Security Classification Conceptual Framework of Space Environment Scientific Data' (2024) 6 (2) Journal of Agricultural Big Data 259, 261 (許琦、胡曉彥、鄒自明等:《空間環境科學數據安全分級概念框架研究》, 載《農業大數據學報》2024 年第 2 期，第 261 頁).

[69] See Chen Bing, Guo Guangkun, 'The Positioning and Rules of Data Classification and Grading System—based on Data Security Law as the Center of Development' (2022) 3 Studies on Socialism with Chinese Characteristics 54–55 (陳兵、郭光坤：《數據分類分級制度的定位與定則——以 < 數據安全法 > 為中心的展開》，載《中國特色社會主義研究》2022 年第 3 期，第 54–55 頁); Zheng Xi, 'Research on Classification and Grading of Criminal Justice Data '(2021) 6 National Procuratorate Journal of Police College 3–6 (鄭曦：《刑事司法數據分類分級問題研究》，載《國家檢察官學院學報》2021 年第 6 期，第 3–16 頁); Shang Xixue , Han Haiting, 'Systematic Construction of Data Classification and Hierarchical Governance Norms' (2022) 10 E-Government 75 (商希雪、韓海庭:《數據分類分級治理規範的體系化建構》，載《電子政務》2022 年第 10 期，第 75 頁).

financial, biological, medical, geographic and other categories of data.[70] In the legislative procedure, we should restrict the authorisation of key data identification, strictly identify the procedure, strengthen the supervision of the identification result, and give the objection right and relief channel to the identification of key data.[71] The second paragraph of Article 21 of the DSL attempts to solve this problem by stipulating that each region and department shall, in accordance with the relevant provisions of the State, determine the key data protection catalogue of their region, department and industry.[72] However, because such provisions are too decentralised, it is easy to cause fragmentation of key data in practice. Therefore, the central state organ should delimit the types and catalogue of key data, and the level of identification agencies in different regions should have uniform standards and restrictions, and be integrated into the coordination mechanism for overall consideration.[73]

C. Legitimacy of Data Governance and Government Power

Data governance is the genus to which the concept of data security belongs, and data security is an important element in data governance. Data governance has the characteristics of being multi-dimensional, multi-level and multi-disciplinary, so it is necessary to build a systematic

---

[70] Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment, Appendix A (Normative Catalogue) refers to identification of key data, and provide guidelines for accrediting bodies and identification standards in oil and gas, coal, petrochemical, electric power, communications, electronic information, iron and steel, non-ferrous metals, equipment manufacturing, chemical industry, national defence industry and other industries, geographic information, special surveying and mapping information, civil nuclear facilities, transportation, postal services, water conservancy, population health, finance, credit information, food safety, statistics, meteorology, environmental protection, radio and television, Marine environment, Certification bodies and identification standards in electronic commerce and other areas.

[71] Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment involves assessment of the political and legal environment of the country or region where the data recipient is located, and includes: a) the assessment content of standard; b) the current laws, regulations and standards in respect of data security in the country or region; c) the mechanism for implementing data security in the country or region, such as the competent authority for cybersecurity or data security, relevant judicial mechanisms, industry self-regulatory associations and self-regulatory mechanisms; d) the legal authority of the national or regional government, including law enforcement, defence, national security, etc., to access and obtain data; e) bilateral or multilateral agreements on data flow and sharing between the country or region and other countries or regions, including bilateral and multilateral agreements on data flow and sharing in law enforcement and supervision.

[72] Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment, Appendix B (Normative Catalogue) Methods for Assessing Security Risks of Personal Information and Key Data Leaving the Country.

[73] In recent years, the Guidelines on Categorisation and Classification of Industrial Data (Trial), Guidelines on Categorisation and Classification of Securities and Futures Industry Data, Technical Specifications for Personal Financial Information Protection and other guidance documents and industry standards issued by various ministries and commissions can be used as a reference for the specific standards for data categorisation and classification of specific industries.

data governance system to avoid the fragmentation of data governance.[74] The legitimacy of the state public power to intervene in data governance depends on the rule of law principle for the exercise of power.[75]

Modern administrative states bear more security obligations, and objectively need to give more power to the state, forming the paradox of regulatory departments in self-authorisation and rule-making. Article 24 of the DSL does not provide procedural provisions for the establishment of a 'data security review system' , and the security review decision is final.[76] Scholars' opinions of the first and second trials of the Draft were not adopted in the final version of the DSL.[77] The non-reviewable, non-litigious and non-judicial review of the final decision of the security review means that the system may exclude ex post facto regulation, which is not only in conflict with the goal of the rule of law, but also inconsistent with the basic principles of public law. Therefore, the final decision of the security review should also be subject to judicial review, and it is necessary to improve the provisions of Article 24, such as the review mode, review organs, start-up conditions, review content, and legal responsibility.

The DSL is an authorisation law with ambiguous powers. In terms of the data security supervision system, Articles 5 and 6 of the DSL delineate

---

[74] See Zuo Xiaodong, 'The Review and Prospect of the Construction of China's Legal Governance System for Data Security' (2023) 23 Governance 32–33 (左曉棟：《我國數據安全法治治理體系建設的回顧與展望》，載《國家治理》2023 年第 23 期，第 32–33 頁); Wang Daofa, Li Jialu, 'The Establishment and Development of Data Security Compliance Standards' (2023) 7 People's Procuratorial Semimonthly 19–20 (王道發、李佳璐：《數據安全合規標準的建立與發展》. 載《人民檢察》2023 年第 7 期，第 19–10 頁).

[75] Technological development requires the guidance of the rule of law. The government shoulders the crucial task of urging the construction of data-related systems and guiding technology towards goodness. With the principle of the rule of law as the bottom line, it sets rules and boundaries for administrative power through the rule of law. See Xie Zhiyong, 'Developing the Digital Government under the Rule of Law from Four Perspectives ' (2023) (01) Journal of Comparative Law 1–3 (解志勇：《數字法治政府構建的四個面向及其實現》，載《比較法研究》2023 年第 1 期，第 1–3 頁); See also Kou Jiali, 'The Construction of Digital Government Cannot Lack the Rule of law' (2022) 9 Economy 40–43 (寇佳麗：《數字政府建設不能缺失法治》. 載《經濟》2022 年第 9 期，第 40–43 頁).

[76] Article 24 of the DSL stipulates: 'The state shall establish a review system for data security, conducting national security reviews of data processing that affects or may affect national security.' Paragraph 2 provides that, 'Security review decisions made in accordance with the law are final decisions.'

[77] Article 22 of the draft establishes the data security review system, but does not clarify the implementing entity, implementation mechanism, review content, etc. of this system. Scholars argued for this provision in both papers and conferences. See Huang, Yuan, Hu, (n 11) 9–13; Digital Rule of Law Research Institute of East China University of Political Science and Law, 'Disputes and Responses in Data Security Legislation' *People's Daily* (Beijing, 31 July 2020) (華東政法大學數字法治研究院：《數據安全立法的爭議與回應》，載《人民日報》2020 年 7 月 31 日) ; See also Future Rule of Law Research Institute of Renmin University of China, 'The Establishment of a comprehensive legal system for data security' *Economic Information Daily* (Beijing, 15 September 2020) （中國人民大學未來法治研究院：《建立完善數據安全法律體系》，載《經濟參考報》2020 年 9 月 15 日).

the division of responsibilities between the central national security leading agency and the national network information department for joint 'coordination'. This may lead to increased overlap in coordination responsibilities within the field of data security between these two entities. It is challenging for various regions and departments to replace the professional supervision provided by data security functional departments, potentially resulting in overlapping or conflicting areas or even vacuums within these functional departments. It is argued that the fragmentation of public data governance is characterised by the failure truly to exert governance effectiveness and fully explore data value, which does not match China's data governance planning.[78] Additionally, many key concepts and systems outlined in this law rely on uncertain legal terminology such as 'national security' and 'public interest', which creates room for arbitrary expansion of public authority power. This does not align with the rule of law concept that emphasises clear authorisation and unified power and responsibility. Therefore, it is suggested that a major administrative decision should be made in the digital age, which involves the participation of multiple stakeholders, dynamic management, and full process supervision policy mechanisms, to establish a data and algorithm security review mechanism, and build an accountability mechanism for administrative personnel, data managers, algorithm developers, and review evaluators.[79]

D. Security and Openness of Government Data

The government is the largest producer and owner of data resources in China, holding more than 80% of the data resources in society.[80] Therefore, the fifth chapter of the DSL consists in a special chapter 'Government data security and openness', which is the first time that China has legislated clearly to regulate government data.

---

[78] See Yuan Zhou, Liu Miaojia, 'The Organizational Law Approach to the Holistic Governance of Public Data——Based on the Development of the National Data Bureau' (2024) 06 Forum on Science and Technology in China 111–112 (袁周、劉苗佳：《公共數據整體性治理的組織法進路——基於國家數據局的展開》，載《中國科技論壇》2024 年第 6 期，第 111–112 頁》.

[79] See Chengbo Jin, Jingwen Wang, 'The Era Landscape of Digital Rule of Law Government: Innovative Governance Tasks, Concepts, and Models' (2022) 236 (08) E-Government 67–73 (金成波、王敬文：《數字法治政府的時代圖景：治理任務、理念與模式創新》，載《電子政務》2022 年第 8 期，第 67–73).

[80] Zhang Feng, 'Government Data Opening and Innovation Development Practice' (*State Information Center/National e-Government External Network Management Center*, 28 Feburary 2020), <http://www.sic.gov.cn/sic/608/612/0228/10419_pc.html> accessed 2 April 2024 (張峰:《政府數據開放與創新發展實踐》，載國家信息中心國家電子政務外網管理中心，http://www.sic.gov.cn/sic/608/612/0228/10419_pc.html，2020 年 2 月 28 日訪問); See Bai Xianyang, 'Research on the Policy System of Open Government Data in the United States' (2018) 2 Research on Library Science 40–44 (白獻陽：《美國政府數據開放政策體系研究》，載《圖書館學研究》2018 年第 2 期，第 40–44 頁).

In terms of the relationship between data security and openness, government data security and government data openness are relevant, but they have their own legislative values and goals which adjust different legal relationships. The purpose and objective of the DSL is to solve the security problems of the state and society involved in the process of data access, collection, storage, transmission and transfer. The openness of government data means that administrative organs open government data to the society in a machine-readable way for individuals and organisations to download and use freely.[81] The legal basis of government data opening is government information opening, which is directly based on the Regulations on Government Information Opening.[82] The legal goal to be achieved is to ensure the citizens' right to know the government data, the right to participate in administrative decision-making, and the right to supervise social governance. Therefore, the DSL should focus on regulating the data security issues in the disclosure of government data and the designation of the corresponding system. A separate 'Government Data Disclosure Law' should be formulated, or the principles and systems for data disclosure should be stipulated in the Regulations on Government Information Disclosure. So, it is not appropriate to stipulate, for instance, 'e-government construction', 'principles and exceptions of government data disclosure' and 'open utilisation of government data' in the DSL. In June 2023, the legislative work plan of The State Council for 2023 proposed to prepare the 'Regulations on Government Data Sharing', which is the latest response of government legislation to this problem.

In terms of data security, the current problem of state agencies obtaining enterprise data at will is more prominent, and the behavior of government data collection should be regulated.[83] Based on data accumulation and iterative updates of algorithm technology, the administrative decision-making mode, governance means, and law enforcement mechanisms are ushering in systematic changes. So the executive has gained enormous digital power. The main question is how

---

[81] 'G8 Open Data Charter' (Cabinet Office, 18 June 2013), <https://www.gov.uk/government/publications/open-data-charter> accessed 15April 2024.

[82] Regulations of the People's Republic of China on the Disclosure of Government Information (Promulgated by Decree No. 492 of The State Council of the People's Republic of China on April 5, 2007 and amended by Decree No. 711 of The State Council of the People's Republic of China on April 3, 2019).

[83] Article 38 of the DSL stipulates that 'Where state organs need to collect or use data to perform their statutory duties, they shall collect or use data within the scope as needed for performance of their statutory duties and under the conditions and procedures provided by laws and administrative regulations'.

to regulate the exercise of that power.[84] The considerations include the following:

First, the principle of legal reservation should be followed. It is necessary to limit the requirement for state authorities to request data from citizens, legal persons and other organisations without the explicit authorisation of laws and regulations. After the implementation of the DSL, it should rationalise and abolish some departmental rules and regulatory documents related to the government's collection of corporate and personal data and information at the level of legal unification. For example, the Departmental Regulation of the People's Bank of China involving keeping customer identity information and transaction records will be invalidated by the implementation of the DSL.[85] In another case, code governance that mainly relies on technologies such as data, code and algorithm models bring human convenience, transparency, and efficiency in life, and the governance capacity and regulatory effectiveness of code in cyber space are the legitimacy basis of code governance.[86] It is argued that this is a pragmatic approach to exploring ways in which both power and technology can work together in a proper way.[87] Conversely, Xizi Wang argued that code governance too can break through the bottom line of the principle of legal reservation. It should be conscious of the dangers of the infringement of the rights of individuals by code governance.[88]

Secondly, the principles of reasonableness and necessity should be followed. The government should collect corporate and personal data under the guidance of reasonable and necessary principles, and avoid

---

[84] See Wang Xizi, 'Digital Governance and Rule of Law: the Rule of Law Constraint of Digital Administration' (2022) 6 Journal of Renmin University of China 17–18 (王錫鋅：《數治與法治：數字行政的法治約束》，載《中國人民大學學報》2022 年第 6 期，第 17–18 頁).

[85] Article 3 of the Measures for the Management of Customer Identification and Customer Identification Information and Transaction Records Preservation of Financial Institutions requires that financial institutions should collect and save customer data information, establish and improve the implementation of customer identification systems: 'Financial institutions shall properly maintain customer identification information and transaction records in accordance with the principles of security, accuracy, completeness and confidentiality, and ensure sufficient reproduction of each transaction to provide the information necessary to identify customers, monitor and analyse transactions, investigate suspicious transaction activities and investigate money laundering cases.'

[86] Professor Lawrence Lessig proposed the proposition of 'Code is Law' in his 'Code and Other Laws of Cyberspace'. The author argued that code is not law. See Xu Donggen, 'The Legitimacy and Validity of Code Governance from the Perspective of Dual Governance' (2023) 1 Oriental Law 36–39 (徐冬根：《二元共治視角下代碼之治的正當性與合法性分析》，載《東方法學》2023 年第 1 期，第 36–39 頁).

[87] See Zhang Quan, Huang Huang, 'Technology Empowerment and Complexity Reduction - An Analysis Based on the "Health Code"' (2022) 2 Research on Political Science 115–124 (張權、黃璜：《技術賦能與復雜性化約——基於"健康碼"的分析》，載《政治學研究》2022 年第 2 期，第 124 頁).

[88] See Wang, (n 84) 17–21.

abusing its power to expand the scope and quantity of data collection. For example, the financial regulatory agency put forward specific requirements for databases,[89] and empowered itself to access the data of the database in real time.[90] In a sense, the broad rationale for anti-money laundering has become a convenient way for financial regulators easily and systematically to access large amounts of personal financial information without restriction, contrary to the principles of rationality and necessity.[91] It is obvious that in the design process, the government embeds its own concepts, values and principles into data processing, algorithm modelling and code writing, which inevitably has certain subjective preferences, and then makes a system design that is favorable to the government's position.[92]

Third, the principle of due process should be followed. In legislation and practice, the conditions under which the government can access corporate or personal data are unclear, often using vague terms such as 'national security' and 'public interest'. Access restrictions should be an important principle that should be implemented in data access practices, however, data sharing may lead to multiple government departments sharing data authorised by laws and regulations to only one department. The DSL stipulates relatively principled procedures for the government to collect data, but lacks provisions to state clearly in writing the object, scope, quantity, purpose, cycle, format and other matters of

---

[89] Article 21 of the Administrative Measures on Anti-Money Laundering and Anti-Terrorist Financing of Internet Financial Institutions (Trial): 'Practitioners shall accept the on-site inspection, off-site supervision and anti-money laundering investigation of the People's Bank of China and its branches in accordance with the law, provide relevant information, data and materials in accordance with the requirements of the People's Bank of China and its branches, and be responsible for the authenticity, accuracy and completeness of the information, data and materials provided.'

[90] Article 16 of the Administrative Measures on Anti-Money Laundering and Anti-Terrorist Financing of Internet Financial Institutions (Trial) : 'For the cash receipts and expenditures of a single or cumulative transaction of more than 50,000 yuan (including 50,000 yuan) and a foreign currency equivalent of more than 10,000 US dollars (including 10,000 US dollars) of a customer on the same day, financial institutions and non-bank payment institutions other than practitioners shall submit a large transaction report within 5 working days after the transaction occurs.'

[91] See Tao Ran, 'Legal Regulations for Systematic Government Access to Corporate Data' (2019) 8 *Masters' E-Journal* (Shanghai Normal University 2019) (陶然：《政府系統性訪問企業數據的法律規制》，上海師範大學 2019 年碩士論文).

[92] From the perspective of the nature of the behaviour, the collection of personal information by administrative organs belongs to the internal administrative procedure and is merely a necessary pre-activity for the subsequent administrative behaviour, and is not subject to the relevant legal restrictions of specific administrative acts. However, as a data collection behaviour, it still needs to follow the principles of legitimate purpose and necessity strictly. See Zhang Linghan, 'The Conflict and Reconciliation between Algorithmic Automated Decision-making and the Administrative Due Process System' (2020) 6 Oriental Law 1 (張淩寒：《演算法自動化決策與行政正當程式制度的沖突與調和》，載《東方法學》2020 年第 6 期，第 4–17 頁).

data submission.[93] As for due process, let us take the CLOUD Act as an example from the perspective of comparative law. Its language leaves many gaps in both the process of developing executive agreements and the procedures for handling individual data demands. First, there is no requirement that the text of the executive agreement be made public before approval by Congress. Second, the process of forming executive agreements also gives the Department of Justice significant power to determine which countries can qualify for agreements.[94] Therefore, it is necessary to issue supporting implementation rules to regulate the procedures of government data collection.

E. Data Sovereignty, Extraterritorial Effect and Impact

Under the trend of demarcating the network boundary of the Internet, the risk brought by the cross-border flow of data has become the focus of all countries, and data jurisdiction is an issue that must be discussed in data legislation.[95] As a further extension of national sovereignty, national data sovereignty is the highest power that a country enjoys over all data within its domain, including the jurisdiction over the use of data, the right to free disposal, the right to exclude harm, and the right to equality of status. In the data era, data security is national security, and data sovereignty is an integral part of national sovereignty.[96]

According to the report, data-localisation policies are spreading rapidly around the world. China is the most data-restrictive country in the world, followed by Indonesia, Russia, and South Africa. Their economies

---

[93] See Liu Ming, 'Suggestions on Improving the DSL (Draft) in "The Mechanism, Expression and Specification of Data Security Legislation"' (2020) 5 Journal of Xihua University (Philosophy and Social Sciences Edition) 21–22 (鄭鉉、汪灝、劉明等: 《數據安全立法的機理、表達與規範——"數據安全法治暨〈數據安全法〉立法研討會發言摘錄》, 載《西華大學學報 (哲學社會科學版)》2020 年第 5 期, 第 21–22 頁).

[94] See Miranda Rutherford, 'The CLOUD Act: Creating Executive Branch Monopoly over Cross-Border Data Access' (2019) 34 Berkeley Tech LJ 1177,1190–1191.

[95] Legislation meant to restrict data flow and information exchange in the name of cybersecurity and sovereignty may have unintended consequences that prevent rather than enable productive use of the Internet. Moreover, nations must ask themselves what real sovereignty in cyberspace is without the ability to maintain and improve mechanisms that allow their citizens and enterprises to benefit from the productive use of the Internet, which depends on rigorous innovation and the global exchange of services and data. See Jing de Jong-Chen, 'Data Sovereignty, Cybersecurity, and Challenges for Globalization' (2015) 16 GEO. J. INT'l AFF, 112.

[96] At present, there is no uniform expression or definition of the concept of data sovereignty. However, in terms of identifying the nature of data sovereignty, it is generally believed that data sovereignty is a new form of national sovereignty in the background of the big data era, and also an important part of national sovereignty. See Report of the 70th Session of the United Nations General Assembly Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. The principle of State sovereignty and the traditional rules of international law related to sovereignty also apply to information and communication technology (ICT) activities carried out by States, which have jurisdiction over ICT infrastructure within their territory.

will all suffer for it. Countries like Australia, Canada, Chile, Japan, Singapore, New Zealand, the United States and the United Kingdom must collaborate on constructive alternatives to data localisation.[97] This area does not admit of so simple a classification. In fact, not only China but also the US and the EU are taking the data restriction policy into account.

In the US, the National Security Law goes beyond the use of one set of tools or body of law. It is cross-disciplinary, encompassing a practical, problem-solving approach that uses all available tools, and draws upon all available partners, in a strategic, intelligence-driven, and threat-based way to keep America safe.[98] Cross-border access to data also raises a set of critical questions about the relationship between territoriality and jurisdiction in an increasingly digitalised world. On the one hand, the location-of-data rule adopted by the Second Circuit provided a strong incentive for mandatory data localisation as a means of controlling governmental access to sought-after data in the *Microsoft Ireland case*.[99] On the other hand, to accept the extraterritoriality of data would require re-thinking the territoriality of the Fourth Amendment principles themselves.[100]

In the EU, clear goals have been set to establish 'digital sovereignty' as the 'main theme of European digital policies'. The European Commission has released 'Shaping Europe's Digital Future',[101] the 'White Paper on Artificial Intelligence'[102] and the 'European Data Strategy'.[103] The digital agenda being formulated by the European Union no longer focuses only on the single market and European standards with global influence, but takes 'technology/digital sovereignty' as its purpose. The Cybersecurity Act passed by the European Union in 2019 laid the legal foundation for

[97] See Nigel Cory, Luke Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them' (Information Technology & Innovation Foundation , 19 July 2021) ,<https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/> accessed 12 April 2024.

[98] See John P Carlin, 'Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats' (2016) 7 Harv Nat'l Sec J 391–6.

[99] See Jennifer Daskal, 'Law Enforcement Access to Data across Borders: The Evolving Security and Rights Issues' (2016) 8 J Nat'l Sec L & Pol'y 473–87.

[100] See Miranda Rutherford, 'The CLOUD Act: Creating Executive Branch Monopoly over Cross-Border Data Access' (2019) 34 Berkeley Tech LJ 1177–82.

[101] See 'Shaping Europe's Digital Future' (European Commission) <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en> accessed 20 April 2024.

[102] See 'White Paper on Artificial Intelligence: A European Approach to Excellence and Trust ' (La Biblia de la IA - The Bible of AI™ Journal, 21 February 2020) <https://editorialia.com/2020/02/21/white-paper-on-artificial-intelligence-a-european-approach-to-excellence-and-trust/> accessed 18 April 2024.

[103] See 'European Data Strategy' (European Commission) <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy> accessed 20 Jun 2024.

the certification of cloud providers within the European Union. Through the cloud project Gaia-X, the independent efforts of strengthening Europe to support small local cloud service providers will be enhanced, creating an interoperable network clearly based on the principle of 'design sovereignty'.[104]

The debate over data flows specifically has recently shifted away from data privacy to different flavours of sovereignty and national security narratives that reflect each nation's respective values and interests, 'digital', 'technological' or 'strategic' sovereignty in the EU and 'cyber' or 'digital' sovereignty in China. While the US criticises the EU's digital sovereignty narrative as protectionist, and China's as a combination of protectionism and authoritarianism, it has recently itself promised an 'emphasis on sovereignty with regard to security, trade, and borders'.[105] Just as in China, the notion of 'sovereignty' is 'deeply entrenched' in the US.[106]

In China's legislation, Article 2 of the DSL emphasises the principle of territorial jurisdiction in the data jurisdiction, Article 2 (2) of the DSL defines the extraterritorial effect of data jurisdiction, which is conducive to the management application and security of the data in the territory. Both of them are in line with the usual practice of the international community in the jurisdiction of national data.[107] In order to cope with the long-arm jurisdiction of overseas law enforcement agencies and to prevent security risks caused by data leaving the country, in the context of cross-border electronic evidence collection the United States has simultaneously disregarded the judicial sovereignty of other countries represented by the data as evidence, as well as the digital sovereignty of other countries represented by the electronic evidence as data.[108] Article 36

---

[104] According to the EUCS certification proposal being developed by the EU's cybersecurity agency (ENISA), cloud service providers will be forced to localise their business and infrastructure within the European Union.

[105] See Tom Ginsburg, 'Authoritarian International Law?' (2020)114(2) American Journal of International Law 221, 259.

[106] See Anu Bradford, Eric A. Posner, 'Universal Exceptionalism in International Law' (2011) (52) Harvard International Law Journal 1, 5.

[107] The Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and the Cross-border Movement of Personal Data, the Asia-Pacific Economic Cooperation (APEC) Privacy Protection Framework, the European Commission's 1995 EU Data Protection Directive through the 2016 General Data Protection Regulation (GDPR), 'Privacy Shield Agreement' signed between the United States and the European Union, etc.

[108] See Zhao Haile, 'On the Conflict and Countermeasures between Cross-border Electronic Evidence Collection in the United States and China's Data Security Legislation' (2024) 1 Journal of Anhui University (Philosophy and Social Sciences Edition) 100–104 (趙海樂：《論美國跨境電子取證與我國數據安全立法的沖突與對策》, 載《安徽大學學報 (哲社版)》2024 年第 1 期, 第 100–104 頁).

of the DSL stipulates an 'approval' procedure.[109] In order further to refine the rules for cross-border data flow, the 'Data Exit Security Assessment Measures' determines the exit supervision mechanism for key law and personal information, and sets a six-month rectification period for data exit activities that have previously occurred. This approach covers key data and personal information. Among them, Article 19 stipulates the principles and methods for the identification of key data. The Provisions on the Standard Contract for the Departure of Personal Information is one of the conditions for exit examination recognised by state authorities signed between domestic data processors and overseas recipients. In addition, the 'Personal Information Cross-border Processing Activities Security Certification Standards' and 'Personal Information Protection Certification Implementation Rules' also set the implementation rules for outbound Chinese data.

However, basing the standard, delimiting the scope of application of the data exit approval rules on whether the data is stored in China may be an overcorrection, contrary to the original intention of the data classification system, and may affect the Chinese data industry's ability to explore overseas markets.[110] Forming a rationalised security level classification before data transmission is an important prevention and control basis for ensuring the safe transmission of related data. Meanwhile, it should also be noted that when sharing the dividend results brought by cross-border data transmission, it is necessary to consider how to unify the classified directories of data prohibited from transmission due to the differentiated development degrees of the digital economy in various countries.[111] In fact, China does not reject the free flow of data.

---

[109] Article 36 states that 'Without the approval of the competent authorities of the People's Republic of China, organisations and individuals in the People's Republic of China shall not provide data stored within the territory of the People's Republic of China to any overseas judicial or law enforcement body.'

[110] In the development of digital trade, the potential threats of cross-border data flow to the interests of enterprises are mainly manifested in two aspects. First, the intellectual property rights condensed in the data may be infringed; second, the collective data interests may not be comprehensively protected. See Ma Qijia, Li Xiaonan, 'Research on Regulatory Rules of Cross-border Data Flow under the Background of International Digital Trade' (2021) 3 International Trade 74–75 (馬其家、李曉楠：《國際數字貿易背景下數據跨境流動監管規則研究》，載《國際貿易》2021 年第 3 期，第 74–75)；Qi Peng, 'The Systematic Coping Logic of Cross-border Risks of Digital Economy Data in the "Belt and Road Initiative" '(2021) 41 05 Journal of Xi'an Jiaotong University (Social Sciences) 104–106 (齊鵬：《"一帶一路"數字經濟數據跨境風險的系統性應對邏輯》，載《西安交通大學學報 (社會科學版)》2021 年第 5 期，第 104–106 頁).

[111] The Russian 'Federal Law' No. 242-FZ (2015) and the 'Personal Data Protection Law of 2015', Article 40, Paragraph 2 of the Indian 'Personal Data Protection Law (Draft)' of 2018, 'Restrictions on Cross-border Transmission of Personal Data', the 'National Policy Framework for E-commerce of India' (Draft), the 'Regulatory Regulations on the Provision of Systems and Electronic Transactions'of Indonesia and the 'Cyber Security Law' of Vietnam in 2019 also insist on establishing localised data centres.

It merely intends to strengthen the control and management of the risks associated with the free flow of data. Judging from the legislative purpose of the DSL, China has already recognised that 'the free flow of data' is the fundamental principle of data flow.[112] Therefore, how to reasonably set up the review rules of cross-border data is very important. The damage caused by restrictions on the free flow of data may be greater than the risk of the free flow of data.[113] According to the classification system, cross-border data approval rules mainly apply to the approval and restriction measures of key data and sensitive data, while for general data, cross-border flow should be protected and promoted.

IV. MAJOR CHALLENGES AND LEGISLATIVE TRENDS FOR THE FUTURE

A. Rebalancing Data Security and Data Freedom

On December 19, 2022, the Central Committee of the Communist Party of China and The State Council issued the Opinions on Building a Data Basic System to Better Play the Role of Data Elements (referred to as the 'Opinions'), which proposed 20 policy measures from four aspects of data: property rights, circulation transactions, income distribution, and security governance (referred to as the 'Data 20' in the industry).[114] In order to implement the spirit of the Opinions, on December 31, 2023, 17 departments, including the National Data Bureau, jointly issued the Three-year Action Plan of 'Data Elements ×' (2024-2026) to give full play to the multiplier effect of data elements and empower economic and social development. It is intended to enhance the level of data supply, improve the data resource system, carry out the construction of industry common data resource libraries, create high-quality training data sets for artificial intelligence large models, guide enterprises to open data, explore the value of business data, and promote the rational utilisation of personal information on the premise of protecting personal privacy; It is further

---

[112] See Tang Qiaoyun, Yang Rongjun, 'The Dual Paradoxes, Operational Logic and Trends of Cross-border Data Flow Governance' (2022) 2 Southeast Academic Journal 72–74 (唐巧盈、楊嶸均: 《跨境數據流動治理的雙重悖論、運演邏輯及其趨勢》, 載《東南學術》2022 年第 2 期, 第 72–74 頁).

[113] Nations are now at a crossroads where they must decide whether enforcing restrictions of data residency and commercial data flows, as well as limiting the freedom of commercial operations within national borders are the most effective ways to protect sensitive information. See Jing de jong- Chen, 'Data Sovereignty, Cyber security, and Challenges for Globalization' (2015) 16 Georgetown Journal of International Affairs 112–122.

[114] 'Opinions of the CPC Central Committee and The State Council on Building a Data Basic System to Better Play the Role of Data Elements' (*Xinhua News Agency*, 19 November 2023) (《中共中央 國務院關於構建數據基礎制度更好發揮數據要素作用的意見》, 載新華社 2023 年 11 月 19 日).

intended to 'optimize the data circulation environment, improve the supportive measures for cultivating data merchants, promote the orderly cross-border flow of data, benchmark against international high-standard economic and trade rules, and continuously optimise the regulatory measures for cross-border data flow.'[115]

On September 28, 2023, the National Cyberspace Administration issued the Regulations on Regulating and Promoting Cross-border Data Flow (Draft for Comment) (referred to as the 'Draft for Comment on Regulating and Promoting'), which aims to further regulate and promote the orderly and free flow of data according to law, reduce data exit security screening obligations with a view to promoting the free flow of data and the development of the digital economy, and unify the implementation of data exit regulations such as the Measures for Data Exit Security Assessment and the Measures for Personal Information Exit Standard Contract. For example, it is clear that when the data generated in international trade, academic cooperation, transnational manufacturing and marketing activities that do not contain personal information or key law are exported, and personal information that is not collected in China is exported, there is no need to declare data exit security assessment, conclude personal information exit standard contracts, and pass personal information protection certification. If it has not been informed by relevant departments or regions or publicly released as key law, the data processor does not need to declare the data exit security assessment as key law.

In recent decades, foreign commentators have raised Network Sovereignty concerns and their impact on data control/transfer within China and across international borders. It is argued that these frequently vague regulations shut foreign information and communications technology (ICT) service providers out of the market and provide an unfair advantage to Chinese firms.[116] There is a kind of claim that true innovation is impossible due to China's censorship and control.[117] On the opposite side, it is argued that after a long period of sustained

[115] 'Data Elements X Three-year Plan (2024-2026)' (*the Chinese Government Network*, 4 April 2024) <https://www.gov.cn/lianbo/bumen/202401/content_6924380.htm> accessed 17 Jan 2024 (《〈"數據要素×"三年行動計畫(2024—2026年)〉發佈》，載中國政府網，https://www.gov.cn/lianbo/bumen/202401/content_6924380.htm，2024年1月17日訪問)..

[116] See Lora Saalman, 'New Domains of Crossover and Concern in Cyberspace' (*Sipri.org*, 26 July 2017) <https://www.sipri.org/commentary/topical-back grounder/2017/new-domains-crossover-and-concern-cyberspace> accessed 8 May 2024.

[117] See Regina M Abrami, William C Kirby and F Warren McFarlan, 'Why China Can't Innovate' (2014) *Harvard Business Review* <https://hbr.org/2014/03/why-china-cant-innovate> accessed 12 Jun 2024.

technocratic success in building a manufacturing powerhouse, China has developed a true innovative spirit.[118] It is too simplistic to focus solely on the impact on innovation combined with Network Sovereignty and related policies in China.[119] In the Chinese context, the distance between the concepts of Network Sovereignty and Data Sovereignty is very small. Controlling online content mainly involves Network Sovereignty, while Data Sovereignty focuses on keeping very valuable data flows safe. Further, the DSL is not an exercise in protectionism, which aims to restrict the foreign competitors and help domestic private firms win. The key concern in the DSL is to maintain the political and social safety of the nation. It is just a by-product of this policy because emphasising data security has a bad influence on digital economic development and technological innovation. And now, there is a very important shift in cross-border data legislation, which means that after several years of data security legislation and practice, China's data security legislation is shifting from focusing on security in the past to promoting and protecting the free flow of data at present and in the future, serving the development of the digital economy, and taking into account data security only in the second place.

However, around the same time, the US House of Representatives unanimously approved the Protecting Americans' Data from Foreign Adversaries Act (H.R.7520 by a vote of 414 to 0.[120] There is no uniform data privacy law at the federal level, and the US Data Privacy and Protection Act (ADPPA), approved by the House Energy and Commerce Committee in July 2022, has been on the legislative calendar in the House of Representatives since then.[121] Act 7520 is the first data privacy bill in US history to come close to completing its legislative journey. The core provision of Act 7520 prohibits US data brokers from transferring sensitive data about Americans to foreign counterparties or entities

[118] The implications of China's shift toward these new productive forces are profound and multifaceted. See Tahir Farooq, 'The acceleration of the development of new-quality productive forces in China has far-reaching and extensive influences' (China Daily Network, 22 March 2020) <http://language.chinadaily.com.cn/a/202403/22/WS65fd4bfea31082fc043be339.html> accessed 20 April 2024; Edward Tse, 'Don't Belittle China's Innovation Potential' (*Europe's World*, 14 February 2014) <https://www.friendsofeurope.org/insights/dont-belittle-chinas-innovationpotential> accessed 20 April 2024.

[119] See Max Parasol, *AI Development and the 'Fuzzy Logic' of Chinese Cyber Security and Data Laws* (Cambridge University Press 2022) 4–6.

[120] Protecting American's Data from Foreign Adversaries Act 2024.

[121] American Data Privacy and Protection Act 2022.

'controlled by or directed by' foreign counterparties.[122] The range of data prohibited from transmission basically covers the 15 categories of 'sensitive data' listed by the ADPPA. In addition, the Foreign Investment Risk Review Modernization Act expands the review authority of the Committee on Foreign Investment in the United States (CFIUS), and imposes stricter regulatory scrutiny on foreign investors' investments in the United States. The Export Control Regulations take relevant cross-border restrictive measures on key technologies of artificial intelligence and sensitive personal data through export control means.[123] If the 7520 Act finally passes all the legislative stages, it will further change the liberal data policy legislation line that the United States has been pursuing, and have a significant impact on China's future data security legislation.

B. Data Security Issues in the Era of Artificial Intelligence

After 2022, the rapid rise of AI technology represented by ChatGPT, showing amazing capabilities and potential, is widely used in finance, medical care, transportation, manufacturing and other fields, and has a profound impact on economic and social development and the progress of human civilisation. At the same time, the potential risks and challenges contained in AI are likely to change profoundly the existing security landscape of countries, enterprises and individuals in the near future. On February 29, 2024, the '2024 Artificial Intelligence Security Report' released by Qianxin found that the malicious use of artificial intelligence technology is growing rapidly, posing a serious threat to political security, cyber security, physical security and military security. AI technology presents two main challenges. The first of these is to amplify existing threats, and the other is to introduce new types of threats, including AI-based deep fake (Deepfake), black generation of large language model infrastructure, malware, phishing emails, fake content and activity

[122] The series of cross-border data transfer policies of the Biden administration highlight the 'national security anxiety' of the United States. See Pan Honglin, Yao Xu, 'The Biden Administration has Issued a Series of Executive Orders, and the Proliferation of Data Security Issues has Become a New Focus' (*Fudan Development Institute*, 7 April 2024)< https://fddi.fudan.edu.cn/_t2515/ 30/c8/c21253a667848/page.htm> accessed 15 April 2024 (潘弘林、姚旭：《拜登政府行政令連發，數據安全議題擴散成為新焦點》，載復旦發展研究院，https://fddi.fudan.edu.cn/_t2515/30/c8/c21253a667848/page.htm，2024 年 4 月 15 日訪問 .

[123] US Congress, 'U.S. Congress Introduces Legislation to Change Foreign Direct Investment Review' (*Jones Day Publications*, 15 November 2017) <https://www.jonesday.com/en/insights/2017/11/us-congress-introduces-legislation-to-change-foreign-direct-investment-review> accessed 17 May 2024.

generation, hardware sensor security and 12 other important threats.[124] In the last couple of years, China became the first country to implement detailed, binding regulations on some of the most common applications of artificial intelligence. These rules constitute the foundation of China's emerging AI governance regime.[125]

1. Large Language Models

Large language models (LLMs) have become more intelligent, and even strong artificial intelligence above average human intelligence has emerged in some fields of research. Many experts around the world have been worried about its security. How to properly use and properly govern the large language model is the key issue that needs to be solved urgently. AI and large language models are inherently associated with security risks. For instance, the application of GPT-4 in healthcare raises ethical concerns that warrant a regulatory framework. Issues such as transparency, accountability, and fairness need to be addressed to prevent potential ethical lapses. Most LLMs have been released globally and no country-specific iterations are available, so that a global approach is required from regulators. It is also not clear what technical category LLMs will fall into from the regulatory perspective. However, based on the differences between LLMs and prior deep learning methods, a new regulatory category might be needed to address LLM-specific challenges and risks.[126]

There has not been enough research and attention from academia and industry on the potential impacts.[127] The world's well-known application

[124] 'Qi'an Xin released the 2024 Artificial Intelligence Safety Report : AI depth counterfeit fraud in 30 times' (Sina Finance , 29 Feburary 2024) <https://baijiahao.baidu.com/s?id=1792217360993401705&wfr=spider&for=pc> accessed 1 Mar 2024 (《奇安信發佈 <2024 人工智慧安全報告 >：AI 深度偽造欺詐激增 30 倍》，載新浪財經，https://baijiahao.baidu.com/s?id=1792217360993401705&wfr=spider&for=pc,2024 年 3 月 1 日訪問).

[125] See Matt Sheehan, 'Tracing the Roots of China's AI Regulations' (*Carnegie Endowment for International Peace*, 27 February 2024) <https://carnegieendowment.org/research/2024/02/tracing-the-roots-of-chinas-ai-regulations? lang=en> accessed 20 May 2024.

[126] See Bertalan Meskó, Eric J. Topol, 'The imperative for regulatory oversight of large language models (or generative AI) in healthcare' (2023) 120 Digital Medicine 1–3; See also Elia Rasky, 'Generative AI Policy in Higher Education: A Preliminary Survey' (2024) Centre for International Governance Innovation 5–8.

[127] On the establishment of artificial intelligence management institutions, we can draw on the experiences of countries such as the United States and Japan of forming 'Ethics Committees for Artificial Intelligence'. See Xiong Jie, Zhang Xiaotong, 'The Data Risks of Generative Artificial Intelligence and its Compliance governance-Taking ChatGtp as Example' (2024) 1 Emerging Rights Collective periodical 44–52 (熊傑、張曉彤：《生成式人工智慧的數據風險及其合規治理 —— 以 ChatGPT 為樣例》，載《新興權利》集刊 2024 年第一卷，第 44–52 頁) ; See also Xiong Jinguang, Jia Jun, 'The Legal Risks and Regulatory Paths Embodied in ChatGPT under the Metaverse' (2023) 2 Emerging Rights Collective periodical 1–12 (熊進光、賈珺：《元宇宙背景下 ChatGPT 蘊含的法律風險及規制路徑》，載《新興權利》集刊 2023 年第二卷，第 1–12 頁); Zhi Zhenfeng, 'The Governance of Information Content of Generative Artificial Intelligence Large Models' (2023) 4 (3) Tribune of Political Science and Law 35–45 (支振鋒：《生成式人工智慧大模型的信息內容治理》，載《政法論壇》2023 年第 4 期，第 35–45 頁).

security organisation OWASP released the top ten security risks of large model applications, including prompt injection, data leakage, insufficient sandbox and unauthorised code execution, which need great attention and active response from the industry. The 'Data Elements X' Three-year Action Plan proposes to support the development and training of large AI models with scientific data. However, there are no laws and regulations on the risk of AI and black language models. The 'Interim Measures for the Management of Generative Artificial Intelligence Services' stipulate that in the process of data annotation in the development of generative artificial intelligence technology, the provider shall formulate clear, specific and actionable annotation rules and carry out data annotation quality assessment. Recently, on April 8, 2024, the National Network Security Standardisation Technical Committee issued a notice for soliciting comments on the draft of the national standard 'Digital Watermarking Technology Implementation Guide', 'Generative Artificial Intelligence Pre-Training and Optimization Training Data Security Specification' and 'Generative Artificial Intelligence Data Annotation Security Specification'.[128] In the future, industry norms and standards for AI enterprise data compliance need to be further improved and refined.

2. Deep Synthesis

China's legislation in this field adopts the principle of 'governance while developing', basically focusing on industry self-discipline, which makes it very difficult to deal effectively with deep synthetic risks. For example, China's 'Provisions on Administration of Deep Synthesis of Internet-based Information Services'[129] stipulates that the editing function of biometric information such as faces and voices should comply with the principle of 'notify-consent' and require compliance with the relevant provisions of the Personal Information Protection Law.[130] For the deep synthesis service providers with public opinion attributes or social mobilisation capabilities, the filing and alternation and cancellation filing procedures shall be performed in accordance with the Provisions on the Management

[128] National Information Security Standardisation Technical Committee: Notice on Soliciting Comments on the Draft of National Standards 'Guidelines for the Implementation of Digital Watermarking Technology for Information Security Technology', 'Security Specifications for Pre-Training and Optimization Training Data of Generative Artificial Intelligence for Information Security Technology', 'Security Specifications for Generative Artificial Intelligence Data Annotation for Information Security Technology', 3 April 2024, https://www.tc260.org.cn.

[129] Article 14 of Provisions on Administration of Deep Synthesis of Internet-based Information Services.

[130] Article 13–18 of The Personal Information Protection Law.

of Internet Information Service Algorithm Recommendation.[131]

The US artificial intelligence strategy has evolved from single-point application to systematic layout, integrating development and security, and delivering a 'combined punch'. It comprehensively demonstrates the ambition of the United States to ensure its leading position in global artificial intelligence at all times, and is highly comprehensive, forward-looking and operational.[132] Deep fake legislation at the federal level in the US includes the Deepfake Task Force Act, which provides for digital identification to reduce the proliferation of deep fakes.[133] The Deep Fakes Accountability Act establishes penal liability by holding video creators accountable for altered videos posted, using digital watermarks to identify malicious deep fakes. Deliberately failing to provide a watermark is an offence punishable by up to five years in prison. Civil penalties of up to $150,000 are imposed for knowingly not providing watermarks for deepfakes.[134] The Deepfakes Report Act requires the Department of Homeland Security to submit a report to Congress on the techniques used to create and detect deepfakes. At the state level, California, Texas, and Virginia have enacted state laws, and Maryland, New York, and Massachusetts are considering their own approaches to legislating on deepfakes.

The rise of deepfakes has brought about a new set of regulatory challenges and considerations. Regulators must meet the moment to provide guardrails for the use of technology as it scales while negotiating the interests of tech companies, arts companies, healthcare, consumers, and other stakeholders.[135] Existing regulations do not clearly define malicious counterfeiting and, from a legislative perspective, it is difficult to distinguish malicious deepfake videos from satire, parody or entertainment. The existing governance often excessively focuses on the output content of deep synthesis, while relatively neglecting governance from other perspectives. Recourse mechanisms, such as takedown notices or legal action, can address copyright questions and defamation.

---

[131] Article 19 of Provisions on Administration of Deep Synthesis of Internet-based Information Services.

[132] See Song Yanfei, Zhang Yao, 'New Trends and Characteristics Analysis of the US Artificial Intelligence Strategic Policy deepfake Task Force' (2024) 02 Artificial Intelligence 7 (宋艷飛、張瑤:《美國人工智能戰略政策新動向及特點分析》，載《人工智慧》2024 年第 2 期，第 7 頁).

[133] Act, S.2559 — 117th Congress (2021–2022).

[134] H.R. 5586-Deepfakes Accountability Act, 118th Congress (2023–2024); H.R.2395-Deepfakes Accountability Act, 117th Congress (2021–2022).

[135] See Dana Cramer, 'Assessing the Near Future of Multi-stakeholder Internet Governance' (2024) Centre for International Governance Innovation 1–4.

More research is needed into the effectiveness of these mechanisms and research into best practices. Standards generally will help shape this conversation. For example, the World Intellectual Property Organization (WIPO) published the 'Draft Issues Paper On Intellectual Property Policy And Artificial Intelligence' in December 2019, which included recommendations for establishing a system of equitable remuneration for victims of deepfake misuse and addressing copyright in relation to deepfakes.[136]

In the future, the regulatory scope can be gradually expanded to the entire chain from information collection to output content of generative AI. Higher requirements should be imposed on large-scale technology developers such as OpenAI, record-keeping of training content, and making it public.[137] Furthermore, the liability clause is relatively sparse and does not specify penalties, and those who violate the provision should be investigated for criminal and administrative responsibilities in accordance with relevant laws and regulations.[138]

3. Face Recognition

In the development of 'Digital China', facial recognition is deeply integrated into fields such as social management, public services, and security guarantees. It has aroused a great deal of criticism and discussion. Some people believe there is no need to be 'terrified' of facial recognition. Facial recognition is the most representative technology in the wave of artificial intelligence, and its development momentum is unstoppable.[139] However, more people are concerned about the risks and regulatory challenges

---

[136] See Amanda Lawson, 'A Look at Global Deepfake Regulation Approaches' (*Responsible AI Institute*, 24 April 2023) <https://www.responsible.ai/a-look-at-global-deepfake-regulation-approaches/> accessed 22 May 2024.

[137] See Zhang Xuebo, Wang Hanrui, 'The legal regulation of generative artificial intelligence' (2023) 6 Shanghai Legal Studies Collective periodical 246–253 (張學博、王涵睿: 《生成式人工智慧的法律規制——以 ChatGPT 為例》, 載《上海法學研究》集刊第 6 卷, 第 246–253 頁).

[138] See Liu Wentao, 'Application Risk and Legal Regulation of AI Face-Changing Technology' (2024) 26 (2) Journal of UESTC (Social Sciences Edition)60–65 (劉文濤: 《AI 換臉技術的應用風險及法律規制》, 載《電子科技大學學報 (社科版) 》 2024 年第 2 期, 第 60–65 頁).

[139] See Qin An, 'There Is No Need to Be Frightened of Facial Recognition', *Beijing Daily* (Beijing, 6 November 2019) (秦安: 《對人臉識別沒必要"談虎色變"》, 載《北京日報》2019 年 11 月 6 日); See also Niu Jin, 'Technological Progress and Privacy Protection Do Not Have to be a Choice Between the Two', Economic Daily (Beijing, 17 December 2019) (牛瑾: 《技術進步不是隱私保護的"天敵"》, 載《經濟日報》2019 年 12 月 17 日).

brought by facial recognition to data privacy and the like.[140] In recent years, China's laws, regulations and national standards on face recognition have emerged in an endless stream. In July 2021, the Supreme People's Court issued the Provisions on Several Issues Concerning the Application of Law to Civil Cases Involving the Use of Face Recognition Technology to Process Personal Information.[141] In October 2022, the state issued the recommended standards 'Security Requirements for Face recognition Data' and 'Technical Requirements for Biometric face recognition Systems', which were implemented on May 1, 2023.[142] In August 2023, the National Cyberspace Administration solicited comments on the 'Regulations on the Application of Face Recognition Technology Security Management (Trial) (Draft for Comment)'.[143] Article 9 of the regulation states:

> Hotels ... [and o]ther business venues, in addition to laws and administrative regulations that should use face recognition technology to verify personal identity, may not handle business, improve the quality of service and other reasons to force, mislead, fraud, coerce individuals to accept face recognition technology to verify personal identity.

The Personal Information Protection Law[144] defines biometric information such as face information as sensitive personal information and puts forward higher protection requirements. According to the law, any unit processing face information should meet the basis of legality: personal consent; necessity for the conclusion or performance of a contract in which one party is an individual; necessity for the implementation of human resources management in accordance with the labour rules and

---

[140] See Zhao Jingwu, 'The Ownership of Rights and Interests and Protection Path of Facial Recognition Information from the Perspective of the "Civil Code"' (2020) 33(05) Journal of Beijing University of Aeronautics and Astronautics(Social Sciences Edition) 21–24 (趙精武：《< 民法典 > 視野下人臉識別信息的權益歸屬與保護路徑》，載《北京航空航太大學學報 (社會科學版)》2020 年第 5 期，第 21–24 頁); Zhou Kunlin , Li Yue , 'Research on the Legal Regulation of Facial Data Application under the Responsive Theory' (2019) 12 Southwest Financial 78–80 (周坤琳、李悅：《回應型理論下人臉數據運用法律規制研究》，載《西南金融》2019 年第 12 期，第 78–80 頁）; Bi Yuqian, Hong Xiao, 'Analysis on the Regulation of Rights Generated by Civil Litigation-Taking the "First Case of Facial Recognition" as the Starting Point' (2020) 3 Law Science Magazine 53–62 (畢玉謙、洪霄：《民事訴訟生成權利規制探析——以"人臉識別第一案"為切入點》，載《法學雜志》2020 年 3 期，第 53–62 頁).

[141] Law Interpretation No. 15 of the Judicial Committee of the Supreme People's Court at its 1841st meeting 2021.

[142] GB/T 41819-2022 Information Security technology face recognition data security requirements 2022; GB/T 41772-2022 Information technology biometric recognition face recognition system Technical requirements 2022.

[143] On the Face Recognition Technology and Safety Management Regulations (Trial) (Draft) Public Notification for Advice 2023.

[144] Article 13 of The Personal Information Protection Law (Order No. 91 of the President of the People's Republic of China, Standing Committee of the National People's Congress 20 August 2021).

regulations formulated according to law and the collective contracts formulated according to law; necessity for the performance of a statutory duty or obligation; necessity to protect the life, health and property safety of natural persons in response to public emergent health events or emergencies; conduct news reporting, public opinion supervision and other acts in the public interest, and process personal information within a reasonable scope; to process, within a reasonable range, information disclosed by individuals themselves or other information that has been legally disclosed; and other circumstances provided for by laws and administrative regulations.

It can be seen that according to the provisions of the current Personal Information Protection Law, the legality standard of 'notify-consent' is very high, and if it is not based on public safety or the performance of statutory duties, there is almost no possibility of the legal processing of facial information. The draft of the 'Management Provisions' also plans to restrict the use of face recognition technology within narrow bounds, and only take laws and administrative regulations as a prerequisite for the use of face recognition. China's laws and regulations generally do not require facial recognition, facial recognition technology is only one of several identity verification technologies. But in reality, facial recognition applications are used widely in many areas.

At present, there is no legal basis for a wide range of facial recognition applications in China. Therefore, future legislation should focus on data flows and legal relationships, the compliance and legal responsibilities of regulatory authorities and operators of public places, clarify the storage, transmission and processing of facial recognition data, and plan adequate alternatives. Recently, it has been a good trend that the policy has been adjusted to cancel mandatory facial brushing in hotels in Shanghai, Hangzhou and other places, and the Ministry of Public Security has issued a document.[145]

C. Formulation of International (Regional) Rules

The generative artificial intelligence represented by large language models has set off a new wave of global artificial intelligence technology development. Issues such as the security and legal boundaries of artificial intelligence-generated content and risk control in the field of artificial intelligence will become the focus of national norms and legislation in

[145] Wu Ruonan, 'Cancel Mandatory Facial Brushing in Hotels! Shanghai, Hangzhou and Other Places Adjusted Their Policies' *Guangzhou Daily* (Guangzhou, 20 April 2024) (吴若楠《取消酒店強制刷臉！上海杭州等地調整政策》，載《廣州日報》2024 年 4 月 20 日).

the future. The 'Recommendation on the Ethics of Artificial Intelligence' was adopted by at the 41st session of the United Nations Educational, Scientific and Cultural Organization (UNESCO) on November 24, 2021, after three years of preparation and consultation.[146] On March 30, 2023, UNESCO issued a statement calling on governments around the world to implement it as soon as possible. Member States should work to develop data governance strategies to ensure the continual evaluation of the quality of training data for AI systems.

On March 21, 2024, the United Nations General Assembly adopted the first global resolution on artificial intelligence, 'Seizing the Opportunities Presented by Safe, Reliable and Trustworthy Artificial Intelligence Systems for Sustainable Development'.[147] The Resolution recognises that data is fundamental to the development and operation of AI systems; it emphasises that fair, inclusive, accountable and effective data governance, improved data generation, access and infrastructure, and the use of digital public goods are essential to harness the potential of secure, reliable and trustworthy artificial intelligence systems for sustainable development, and urges Member States to share data governance best practices and promote international cooperation, collaboration and assistance in data management, to improve the consistency and interoperability of approaches where feasible, to facilitate the trusted cross-border data flow of secure, reliable, and trusted AI systems, making their development more inclusive, equitable, efficient, and beneficial to all.

The declaration and initiative issued by the World Trade Organization put forward the vision of establishing globally unified standards and rules for cross-border data flows, providing a principled framework for the establishment of international rules in the future, advocating the integration of digital trade and the internationalisation of rules through trade agreements. In 2020, the World Economic Forum proposed five goals of technology trade (The 5 Gs), which put forward

[146] Recommendation on the Ethics of Artificial Intelligence of the General Conference of the United Nations Educational, Scientific and Cultural Organization (UNESCO) 2021.

[147] 'United Nations General Assembly Adopts Resolution on Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development (Office of The Spokesperson, 21 March 2024) <https://www.state.gov/united-nations-general-assembly-adopts-by-consensus-u-s-led-resolution-on-seizing-the-opportunities-of-safe-secure-and-trustworthy-artificial-intelligence-systems-for-sustainable-development/> accessed 10 Jun 2024. This resolution builds on multiple international initiatives to articulate a shared approach to safe, secure, and trustworthy AI systems, including the Bletchley Declaration from the UK Safety Summit, the Global Partnership on AI (GPAI) Summit hosted by India in 2024, the International Code of Conduct for Organisations Developing Advanced AI Systems developed through the G7 Hiroshima AI Process hosted by Japan in 2023, the G20 Principles for Trustworthy AI, and the OECD AI Principles.

principled suggestions for cross-border data transmission. Part of Global Data Transmission and Responsibility Framework pointed out that trade digitalisation requires the establishment of a globally accessible, affordable, and swiftly-connected, legal and reliable data transmission framework that crosses national borders in a trustworthy manner. The development of technologies such as artificial intelligence, blockchain, and the Internet of Things also requires the reduction of obstacles to cross-border data flows.[148] At present, there are no unified international standards and rules for the cross-border flow of data. These declarations and initiatives only have the effect of suggestions in terms of validity.[149] On January 19, 2024, the European Commission, the European Parliament and the Council of the European Union jointly finalised the Artificial Intelligence Act, which is of extraordinary importance for the development of artificial intelligence and the digital economy worldwide. Together with the EU Data Act, Data Governance Act (DGA) and General Data Protection Regulation (GDPR), it will have an important impact on the international rules of data governance in the field of artificial intelligence.

Since 2010, regional trade agreements have played an important role in integrating e-commerce and digital trade provisions. Some important regional trade agreements have stipulated regulatory requirements for cross-border data flows. The Trans-Pacific Partnership Agreement (TPP) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) take data freedom as the basic principle of the cross-border data rules.[150] Conversely, the Regional Comprehensive Economic Partnership (RCEP) is different from the fundamental rights model of the EU and the data privacy model of the United States. RCEP member states have reflected the interests and demands of developing countries more in the construction of data flow rules, and for the first time stipulated the principle of data localisation in regional trade agreements, which has a significant impact on the changes in the existing

---

[148] See Dr. Javier Lopez Gonzalez, 'Trade and cross-border data flows—Mapping the policy environment and thinking about the economic implications' (WTO Trade Dialogues, 2020). See also 'The Promise of Trade Tech-Policy Approaches to Harness Trade Digitalization', (World Economy Forum 2020).

[149] See Mira Burri, *Big Data and Global Trade Law* (Cambridge University Press, 2021) 83–112; Nivedita Sen, 'Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?' (2018) 21 (2) Journal of International Economic Law 323–348.

[150] 'Overview and Issues for Congress, IF12078 · VERSION 6' (CPTPP, 16 June 2023) <https://crsreports.congress.gov.> accessed 28 April 2024;'CPTPP Text and Associated Documents' (Australian Government/ Department of Foreign Affairs and Trade) <https://www.dfat.gov.au/trade/agreements/in-force/cptpp/official-documents> accessed 28 April 2024.

regulatory pattern of global cross-border data flows.[151]

International agreements formulated by global and regional international organisations are at risk of inefficiency and uncertainty, and it is difficult to meet the urgent need for cross-border data rules in the development of the digital economy. So far, Hong Kong has signed eight free trade agreements respectively with the Chinese mainland, New Zealand, the European Union, Chile, Macao, the Association of Southeast Asian Nations (ASEAN), Georgia and Australia. The regional trade agreements signed by Hong Kong and the RCEP will produce legal conflicts in their application and enforcement. For example, Hong Kong negotiated cross-border data clauses with Australia in the Australia-Hong Kong Free Trade Agreement (AUHKFTA). In Chapter 11, in the e-commerce section, it covers cross-border data rules, including those related to electronic signatures and electronic authentication, the legal framework for electronic transactions that is consistent with the principles of the UNCITRAL Model Law on Electronic Commerce of 1996 or the United Nations Convention on the Use of Electronic Communications in International Contracts of 2005, freedom of information flow including financial services, the prohibition of the localisation of computing facilities including financial services, and personal information protection, etc.[152]

Hong Kong and Macao have their own rules on cross-border data flows. In December 1996, the Personal Data (Privacy) Ordinance was implemented in Hong Kong. In 2021, the Legislative Council of the Hong Kong Special Administrative Region passed the Personal Data (Privacy) (Amendment) Bill. The 'Cross-border Data Transfer Ordinance' and 'Cross-border Data Transfer Guidelines' of Hong Kong stipulate three scenarios of data transfer. Hong Kong belongs to the common law system and tends to follow the minimum data supervision model of the United States for personal information protection, emphasising the autonomy of market entities, and believing that the government should adopt a minimum

---

[151] See Hong Zhihang, Huo Junxian, 'RCEP's Regulations on Cross-border Data Flows and its Important Impacts' (2022) 4 Southwest Finance 83 (洪治綱、霍俊先：《RCEP 對數據跨境流動的規制及其重要影響》，載《西南金融》2022 年第 4 期，第 83 頁); Ma Haitong, 'RCEP Cross-Border Data Flows: A Review of the Rules and China's Response' (2024) 6 Foreign Economic Relations & Trade 30–31 (馬海桐：《RCEP 跨境數據流動的規則檢視與中國因應》，載《對外經貿》2024 年第 6 期，第 30–31 頁).

[152] Free Trade Agreement between Hong Kong, China and Australia 2018.

supervision policy.[153] Macao enacted the 'Personal Data Protection Law' in 2005. Macao belongs to the civil law system. This bill has drawn on and absorbed the principles and contents of the EU's GDPR, and is highly systematic and rigorous.[154] There are significant differences between the mainland, Hong Kong and Macao in terms of basic conceptual categories, legal bases for processing personal information, sensitive information, obligations of processors and legal responsibilities. The data classification standards of Guangdong, Hong Kong and Macao are not yet clearly unified, which may lead to fragmentation of the scope of key law and make it difficult to implement the restrictions and censorship systems effectively on the cross-border transmission and flow of core data and key law in the Greater Bay Area.[155] Therefore, on the basis of the types and catalogues of key law defined by the state, the identification agencies, classification standards and procedures for key law in the Greater Bay Area should be unified and taken into overall consideration by the coordination mechanism. First, it is necessary to raise the level of data legislation in the Greater Bay Area, to adopt a top-level design legislative model, and to integrate the advantages of the current laws of the three regions of Guangdong, Hong Kong and Macao. Second, the experience of legal integration of international organisations, regional nation alliances and federal countries can be drawn on, in order to introduce a unified model law for data security and information protection in Guangdong, Hong Kong and Macao. Third, it needs to establish a Guangdong-Hong Kong-Macao legislative coordination working institution led by the Central Leading Group for Guangdong-Hong Kong-Macao Work, and a Guangdong-Hong Kong-Macao legislative coordination working mechanism. Comprehensively considering the level of data information security and protection in the three regions and the actual needs of cross-border data flow in the Greater Bay Area, this group should jointly negotiate and determine the general and exceptional principles, legislative

---

[153] See Zhang Hongrong, 'Guangdong-Hong Kong-Macao Greater Bay Area Cross-border Data Flow and Transaction: The Approach of Conflict of Laws and Institution' (2023) 6 Journal of Guangdong Open University (張洪榮：《粵港澳大灣區跨境數據流通交易：法律沖突與制度進路》，載《廣東開放大學學報》2023 年第 6 期).

[154] See Yang Aoyu, 'The Text and Practice of the Personal Data Protection Law of the Macao Special Administrative Region' (2017) Southwest University of Political Science and Law 1 (楊翱宇：《澳門特別行政區個人資料保護法的文本與實踐》，西南政法大學 2017 年碩士畢業論文，第 1 頁).

[155] See Feng Zehua , Liu Zhihui, 'Cross-border Flow of Financial Data in Guangdong-Hong Kong-Macao Greater Bay Area: Practical Issues and the Way Forward for the Rule of Law' (2024) 5 Journal of Financial Development Research 67 (馮澤華、劉志輝：《粵港澳大灣區金融數據跨境流動：現實問題與法治進路》，載《金融發展研究》2024 年第 5 期，第 67–76 頁).

framework and reserved provisions of legislation, and form a model text of data and information laws in the Greater Bay Area.[156]

At present, some regions in China are deeply promoting the pilot of cross-border data transfer security management.[157] At the same time, in order to implement the 'Memorandum of Cooperation on Promoting Cross-border Data Flow in the Guangdong-Hong Kong-Macao Greater Bay Area' on the cooperation measures of 'jointly formulating and organising the implementation of cross-border Personal information standard contracts in the Guangdong-Hong Kong-Macao Greater Bay Area, and strengthening the record management of cross-border personal information standard contracts', The Cyberspace Administration of China and the Hong Kong Bureau of Innovation, Technology and Industry should jointly formulate the 'Guidelines for the Implementation of the Standard Contract for the Cross-border flow of of Personal Information in the Greater Bay Area (Mainland and Hong Kong)',[158] to promote cross-border data flow and regulation in the Greater Bay Area.

V. CONCLUSION

Data is the basic production factor of social and economic development in the era of artificial intelligence, and a correct understanding of the relationship between data security and development is of great significance to both of them. In the context of the overall national

---

[156] See Feng Anqi, Lin Guoqing, Wang Luqi, Shen Xinyue, 'Analysis of the Governance System for Cross-border Transactions of Data Elements: Taking the Guangdong-Hong Kong-Macao Greater Bay Area as an Example' (2024) 27 (10) China Management Informationization 114, 117 (馮安琪、林國清、王璐琪等：《數據要素跨境交易治理體系探析 —— 以粵港澳大灣區為例》，載《中國管理信息化》2024 年第 10 期，第 117 頁); Yang Xiaowei, Zhang Yuxin, Jia Dan, 'Research on Challenges and Countermeasures of Cross-border Data Flow in Guangdong-Hong Kong-Macao Greater Bay Area' (2023) 4 Industry Information Security 73, 78 (楊曉偉、張譽馨、賈丹：《粵港澳大灣區數據跨境流動的挑戰與對策研究》，載《工業信息安全》2023 年第 4 期，第 78 頁).

[157] Beijing Digital Trade Pilot Zone, Shanghai Free Trade Zone Lingang Area, Hainan Free Trade Port, (Zhejiang) Free Trade Pilot Zone and other places have explored the relevant 'data cross-border pilot work'. They encourage some free trade ports and free trade zones to be 'pilot', support Hainan, Shanghai, Beijing, Zhejiang, Shenzhen and other domestic regions where the conditions are better for improving the rules in the 'stress test', breaking through exploration of cross-border data property rights transactions, and taking the lead in joining the international regional data free flow system arrangements.

[158] Announcement of the Hong Kong Bureau of Innovation, Technology and Industry and Cyberspace Administration of China No. 3, 2023, "Guidelines for the Implementation of the Standard Contract for the Cross-border Flow of Personal Information in the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland and Hong Kong)"' (State Council of People's Republic of China, 10 December 2023) <https://www.gov.cn/zhengce/zhengceku/202312/content_6920259.htm> accessed 12 Jun 2024 (《粵港澳大灣區（內地、香港）個人信息跨境流動標準合同實施指引》，載中國政府網，https://www.gov.cn/zhengce/zhengceku/202312/content_6920259.htm，2024 年 6 月 12 日訪問).

security concept and the strengthening of data security legislation and practice in various countries, China adopts a state-led data governance model, strives to practice the rule of law, and passes on its data security concepts, legislative principles, and system design to the world. In the future, it is necessary to maintain continuous attention to the potential risks and impacts of the development of digital society and to provide timely support in terms of institutions and regulations. China needs actively to participate in the formulation of international rules for data regulation of cross-border data flows, and to explore joining regional institutional arrangements for cross-border data flows, promote bilateral and multilateral consultations on data governance, establish mutually beneficial rules and other institutional arrangements, and encourage the exploration of new ways and models for cooperation. Efforts should be made to increase the contribution of Chinese wisdom to international data governance and the establishment of a global data rules system, the promotion of strengthening information exchange, and technical cooperation in artificial intelligence governance. Overall, the international community has yet to reach a consensus on the data sovereignty principle. Facing the future, how to promote an international community consensus, and how, given the shared premise of respecting data sovereignty, to establish mechanisms and standards for international data flow, openness, and sharing, so that data can become information technology achievements shared by all mankind, are common issues that need to be urgently faced and solved in the future.

Professor of Law, College of Humanities and Social Sciences,
Harbin Engineering University, 145 Nantong Street, Nangang District, Harbin, China.
Email: dingwei6262@163.com