Post-print: A Study on the Coordination between the Data Security Law and the Archives Law

Authors: Wang Yujue, Wu Yinuo, Ling Minhan

Date: 2023-04-01T00:00:00+00:00

Abstract

[Purpose/Significance] This paper analyzes the respective emphases and mutual intersections of the Data Security Law and the Archives Law regarding their objects of regulation, legislative purposes, and legislative principles, explores the necessity and feasible pathways for promoting the coordinated development of the two laws, and provides references for subsequent legislation on archives and data.

[Method/Process] Through literature research and comparative analysis, it identifies the problems faced in the coordinated advancement of the Data Security Law and the Archives Law, and proposes recommendations for the formulation of supporting subordinate legislation for the two laws by drawing on extraterritorial experiences.

[Results/Conclusion] The study finds that, proceeding from their respective management practices, the two laws exhibit insufficient coordination in legal regulation concerning provisions on archives and data protection, classification standards for archives and data, and cross-border flow of archives and data, resulting in some data falling into a “gray area” where data security cannot be guaranteed. The article proposes that: the participation of archival departments in data governance should be clarified; classification standards for data and archives conforming to China’s realities should be established from the perspective of continuity in long-term data preservation; archival departments and data departments should collaboratively establish laws, regulations, and management mechanisms for the cross-border flow of important data; and the provisions on personal privacy protection in the two laws should be improved.

Full Text

A Study on the Harmonization of the Data Security Law and the Archives Law

Wang Yujue[1], **Wu Yinuo**[1,2], **Ling Minhan**[1] [1]School of Information Management, Wuhan University, Wuhan 430072 [2]National Demonstration Center for Experimental Library and Information Science Education, Wuhan University, Wuhan 430072

Abstract: *[Purpose/Significance]* This study analyzes the respective emphases and intersections of the Data Security Law and the Archives Law in terms of regulatory objects, legislative purposes, and principles, exploring the necessity and feasible pathways for promoting the coordinated development of these two laws to provide references for subsequent legislation on archives and data. *[Method/Process]* Through literature review and comparative analysis, this paper identifies the main problems in the coordinated advancement of the Data Security Law and the Archives Law, and proposes recommendations for formulating supporting subordinate legislation by drawing on foreign experiences. *[Result/Conclusion]* The study finds that, starting from their respective management practices, the two laws exhibit insufficient coordination in legal regulations concerning archives and data protection, classification standards for archives and data, and cross-border flow of archives and data, resulting in some data falling into a "gray area" with no guarantee of data security. The article proposes that the participation of archival departments in data governance should be clarified; classification standards for data and archives consistent with China's actual conditions should be established from the perspective of long-term data preservation continuity; archival and data departments should collaboratively establish laws, regulations, and management mechanisms for the cross-border flow of important data; and the content related to personal privacy protection in both laws should be improved.

Keywords: Data Security Law; Archives Law; data security; archives legislation; data legislation

---

Introduction

On June 18, 2020, the 19th meeting of the Standing Committee of the 13th National People's Congress passed the revised Archives Law of the People's Republic of China (hereinafter referred to as the Archives Law), which took effect on January 1, 2021. The Archives Law improves and perfects the archives management system across all stages including collection, arrangement, protection, utilization, and supervision, and adds a special chapter on "Archives Informatization Construction" to address new circumstances and challenges facing archival work in the big data era. Subsequently, on July 3, 2020, the draft Data Security Law of the People's Republic of China (hereinafter referred to

as the Data Security Law) was released for public comment, officially launching China's first specialized legislation in the field of data security. After three rounds of deliberation and revision, on June 10, 2021, the 29th meeting of the Standing Committee of the 13th National People's Congress passed the Data Security Law of the People's Republic of China, which took effect on September 1, 2021.

As early as 2017, General Secretary Xi Jinping emphasized the need to effectively safeguard national data security, strengthen the overall coordination of policies, supervision, and laws, and accelerate the construction of regulatory systems [1]. Upon the release of the Data Security Law draft, numerous scholars including Zhai Zhiyong [2], Zhang Meng [3], Liu Guifeng [4], Ma Zhongfa [5], and Xu Jiujiu [6] discussed the coordination between the Data Security Law and other laws such as the National Security Law, Cybersecurity Law, and Personal Information Protection Law. With the application of emerging technologies like big data, cloud computing, cloud storage, and the Internet of Things in digital archives construction, government information openness, and smart archival services, "archival datafication" research has become a new paradigm for archives informatization in the artificial intelligence era [7]. The archival community has gradually recognized that data governance represents a new perspective and function for archives management in the big data era [8], proposing new concepts such as "archival domain data ontology" [9] and "record factors" [7].

Concurrently, questions such as "whether archives belong to data," "the relationship between the Data Security Law and the Archives Law," and "the impact of the Data Security Law on archival theory and management practice" have attracted attention from both the judicial community and the library and information science field. Professor Gao Fuping of East China University of Political Science and Law proposed at the Data Security Law Draft and Data Rule of Law Seminar in July 2020 that to achieve dual objectives of domestic and international dimensions, the institutional measures for data security in the Data Security Law should be coordinated and connected with those in the Cybersecurity Law, Archives Law, and other laws [10]. Deng Lingbin suggested that the release of the Data Security Law provides strong legal protection for data security in China's library and information science community [11]. Jin Bo et al. proposed that establishing and improving the archival data regulatory system is an important means to ensure archival data security [12]. Geng Zhijie et al. called for accelerating the legislative connection between the newly revised Archives Law and laws such as the Data Security Law, Law on Guarding State Secrets, and Cybersecurity Law, and formulating management regulations for the cross-border internet transmission of archival data [13]. Ding Jiayou et al. explored new challenges to archival data security under the overall national security concept, the Archives Law, and the Data Security Law [14].

Data processing and archives management represent the front-end and back-end of data management activities, respectively. They overlap in management objects and complement each other in management processes, jointly committed to

protecting data security. However, the current Data Security Law and Archives Law lack attention to macro-level data governance and require further coordination and 磨合 in areas such as data security protection, data classification, cross-border flow of important data, and personal privacy protection. Therefore, exploring existing problems in the coordinated development of the Data Security Law and the Archives Law is of great significance for implementing existing laws, formulating supporting regulations, and systematically constructing a comprehensive data security governance system, which constitutes the foundation of this study.

Current research has focused on the coordination between the Data Security Law and related laws such as the Cybersecurity Law and Personal Information Protection Law. However, scholars in library, information, and archival science have insufficient participation in coordination studies of data security-related laws, with few research results exploring the coordination between the Data Security Law and laws such as the Public Library Law, National Intelligence Law, and Archives Law. This article attempts to conduct a coordination study of the Data Security Law and the Archives Law, examining the internal logic and practical dilemmas of their coordinated development, and discussing their coordination in "data protection," "classification of important data," "cross-border flow of archives and data," and "privacy protection of personal data," aiming to provide references for the connection and coordination between legislation in library, information, and archival fields and data legislation.

---

2. Internal Logic of Coordination Between the Data Security Law and the Archives Law

Clarifying the conceptual overlap between "data" and "archives" in legal theory, analyzing the similarities and differences in legislative purposes and principles between the Data Security Law and the Archives Law, and examining their mutual reinforcement constitute the logical starting point for coordinating the two laws and improving supporting subordinate legislation.

2.1 Overlapping and Interconnected Regulatory Objects From a legal conceptual perspective, the regulatory objects of the two laws exhibit overlap and interconnection. Unlike the Cybersecurity Law, which defines "network data" as "various electronic data collected, stored, transmitted, processed, and generated through networks," the Data Security Law defines "data" as "any record of information in electronic or other forms," thereby on the surface including paper archival information and other written records within the scope of data [15]. The Archives Law defines "archives" as "various historical records in different forms such as text, charts, audio-visual materials, etc., directly formed by state organs, social organizations, enterprises, public institutions, and other organizations as well as individuals in economic, political, cultural, social, ecological civilization, military, foreign affairs, scientific and technological activities,

which have preservation value for the state and society." Meanwhile, countries such as France, the United Kingdom, the United States, and Canada emphasize that the concept of "archives" is not limited by form (time, format, carrier, etc.), as shown in Table 1 .

In the big data era, the transition of archival management practice from dual-track to single-track systems and from dual-set to single-set systems will also promote coordination between archives and data legislation. The Archives Law adds a chapter on "Archives Informatization Construction," making targeted provisions for the secure preservation and effective utilization of digital archival resources. The "archival digital resources" mentioned encompass electronic archives, digitized traditional carrier archives, and other digital resources with archival attributes or value. In other words, all data with archival attributes generated in various systems are considered. Therefore, at the conceptual level, both "data" and "archives" are broadly "records," with overlapping coverage. The conceptual connotations of archives and data are converging and gradually integrating.

From the perspective of generating subjects and value forms, both include institutions, enterprises, and individuals as generating subjects. Data is the "record" naturally formed by relevant departments, industry organizations, enterprises, and individuals during data activities, emphasizing immediacy and serving as the basic condition for business operations. Archives are "historical records" formed by current and past institutions, organizations, enterprises, public institutions, and individuals that have been appraised as having preservation value for the state and society, emphasizing diachronicity. In essence, "archives" are "data" that have been appraised as having long-term preservation value for the state and society. Meanwhile, with the flourishing digital environment, the boundaries between archives, documents, information, and data are increasingly blurred. Many information carriers such as databases and web pages cannot strictly meet traditional definitions of archives but have high preservation value [17], making "data state" a new form of archival existence.

2.2 Complementary Legislative Purposes and Principles The successive enactment of the Archives Law and the Data Security Law represents China's legislative response to global data explosion and the archives work landscape characterized by "digitizing existing archives and electronicizing new additions." In terms of legislative purposes, the two laws regulate data security management activities from different dimensions—data processing and archives management—jointly implementing the requirements of the overall national security concept. The Data Security Law elevates data security to the national strategic level, with the legislative purpose of "regulating data processing activities, safeguarding data security, promoting data development and utilization, protecting the legitimate rights and interests of individuals and organizations, and safeguarding national sovereignty, security, and development interests." The data security it maintains is defined as "ensuring data is in a

state of effective protection and lawful utilization through necessary measures, and possessing the capability to guarantee continuous security," focusing on security in current data processing activities (collection, storage, use, processing, transmission, provision, disclosure, etc.).

The legislative purposes of the Archives Law include three aspects: strengthening archives management, improving archives informatization construction, and serving the cause of socialism with Chinese characteristics. Its requirements for archives security are mainly stipulated from two dimensions: physical security and information security. Physical security refers to the security of archival carriers or storage media; information security means that the authenticity, integrity, reliability, and security of archives are not compromised, and that relevant confidentiality provisions are not violated during archives opening and utilization [19]. Additionally, the Archives Law emphasizes the standardization of management activities such as archives collection, arrangement, protection, utilization, and supervision, as well as the security of archival entities and information during permanent or regular preservation.

In terms of legislative principles, both laws follow the basic legislative principles established by the Legislation Law of the People's Republic of China while also reaching consensus on professional legislative principles such as balancing security and utilization promotion and consistency of rights and responsibilities. Specifically, the Data Security Law adopts principles including balancing data security protection with data development and utilization (Articles 1 and 13), coordinated governance of data security work (Articles 5, 6, 9, 17, and 18), consistency of rights and responsibilities (Chapter 4 on data security protection obligations), and safeguarding data sovereignty (Articles 1, 25, 26, 36, etc.) [4]. After more than thirty years of archival legislative practice since the first Archives Law in 1987, the Archives Law adheres to principles including the leadership of the Communist Party of China over archives work (Article 3), unified leadership and tiered management of archives work (Article 4), maintaining archives integrity and security (Articles 1, 4, 19, 35), balancing archives utilization rights and protection obligations (Articles 1, 4, 5), and parallel rewards and punishments (Articles 7, 48, 49, 50, 51).

2.3 The Archives Law's Specific Requirements for Long-Term Data Security Preservation The Archives Law's requirements for long-term preservation security align with the Data Security Law's requirement for data security to have "the capability to guarantee continuous security." The Archives Law's statutory requirements for electronic archives and practical measures such as backup, migration, monitoring, log management, and audit trails for long-term preservation of digital archival resources provide references for standardizing data processing procedures, establishing secure data processing models, and promoting coordinated full-process control between the Data Security Law and the Archives Law. By the end of 2020, national comprehensive archives at all levels held 1,387.5 TB of electronic archives, including

390.2 TB of digital photos and 523.5 TB of digital audio and video recordings, plus 19,588.5 TB of digitized archival materials [20]. As digitization of paper archives continues to improve and the number of born-digital documents grows rapidly, the objects of archival work are quickly shifting from "paper archives" to "electronic documents" (electronic archives).

Article 37 of the revised Archives Law stipulates that electronic archives should be "reliably sourced, procedurally standardized, and element-compliant" to ensure their authenticity, integrity, availability, and security. Article 39 proposes off-site backup for important electronic archives, covering not only the electronic archives themselves but also, based on data recovery and effective utilization needs, metadata, configuration files, and log files of electronic archives management information systems. This imposes requirements from the back-end of archives management on data management system software, full-process and full-element preservation of data, whole-process control of data processing, and data understandability and traceability.

2.4 The Data Security Law Provides New Approaches for Improving Archives Security Management Systems From the perspective of data security protection continuity, the Data Security Law provides new ideas and directions for archival departments to establish and improve archives security management systems. Chapter 3 of the Data Security Law, "Data Security Systems," covers data classification and tiered protection (Article 21), data security risk assessment (Article 22), data security emergency response (Article 23), data security review (Article 24), data export control (Article 25), and other aspects, aiming to establish normalized, full-process data security management systems. Archives security is the lifeline of archival work, facing non-traditional security issues such as data storage, archives transmission, and system operation and maintenance in the big data era. However, the Archives Law's provisions on safeguarding archives security are scattered across chapters on archives management, archives informatization construction, supervision and inspection, and legal liability, covering mechanisms for improving archives security work (Article 19), physical archives security (Article 19), archives information security (Article 35), remediation of security hazards (Articles 44 and 45), and strict legal liability (Article 48), lacking overall principles, foundation, and coherence. The Data Security Law's provisions on data security risk monitoring and assessment, emergency response, and regulation provide ideas for improving archives security management systems.

Simultaneously, the Data Security Law provides legal support for archival departments to obtain an "identity" in data management. For a long time, archival departments have often been in a state of "voicelessness" and "absence" in data management. As the final preservation department for important data, the construction of top-level standards for data governance directly affects the formulation of subsequent archives management standards and ultimately determines the effectiveness of archives development, utilization, and safe custody. Multi-

ple provisions in the Data Security Law (Articles 5, 6, 9, 17, and 18) regarding the establishment of a national data security work coordination mechanism, data security supervision, and promoting industry organizations to formulate data security behavior norms and participate in standard-setting provide legal support for archival departments to participate in collaborative data security governance.

---

3. Current Problems in Coordinating the Data Security Law and the Archives Law

Currently, both the Data Security Law and the Archives Law proceed from their respective management practices, resulting in insufficient institutional coherence between front-end data processing and back-end archives management. The legal regulations lack coordination in provisions on archives and data protection, classification standards, and regulatory subjects for cross-border flow, which can compromise data integrity, availability, and security.

3.1 Inadequate Provisions on Archives and Data Protection Archives security is an important component of data security, providing guarantees for long-term data preservation. Currently, compared with the Data Security Law, the Archives Law still lacks specific provisions on archives classification and tiered protection, archives security risk monitoring, assessment, early warning, and security review, focusing more on remedial measures after security hazards and accountability for failure to take remedial measures. Moreover, the Archives Law's regulatory objects focus on archives management practice itself, lacking analysis and concern for the overall national legal framework and the macro context of data or information management, which can lead to insufficient recognition of the legitimacy of archival departments' participation in collaborative data security governance.

Regarding the Data Security Law, on one hand, once data is tampered with, destroyed, leaked, or illegally obtained and utilized, it can cause great harm to national security, public interests, or the legitimate rights and interests of organizations and citizens. Although the Data Security Law, following the Cybersecurity Law, imposes higher protection requirements for important data, subsequent legislation needs to further clarify the data security responsible person, management institution, risk assessment subject, report recipient, assessment frequency, etc. On the other hand, data management faces challenges such as system vulnerabilities, password leaks, and hacker attacks, with increasingly high requirements for the physical and system security of data storage. How to ensure data security has become an important issue in the big data era. The Data Security Law defines the scope of data processing as data collection, storage, use, processing, transmission, provision, and disclosure. However, data "protection," which is closely related to data security and represents both the terminal activity of data processing and a requirement for the entire data pro-

cessing process, is not included in "data processing," nor is specific responsibility for data protection clearly assigned. This excludes data "protection" from the law's scope of application at the conceptual level, separating data from archives and the Data Security Law from the Archives Law, which can easily lead to insufficient data reliability and incomplete or lost content, structure, and contextual information of electronic archives.

3.2 Uncoordinated Classification Standards for Archives and Data
Existing data and archival legislation employs different classification methods due to different management systems. Archives classification emphasizes institutional fonds, while data classification is based on business scope [21], making unified classification standards unnecessary. Therefore, this paper examines existing legal provisions on data and archives classification from two aspects—system-level protection and content-level protection—emphasizing consensus on ensuring data security, as shown in Table 2 .

From the system-level protection perspective, Article 27 of the Data Security Law connects with the Cybersecurity Law, clearly stipulating that data processing activities should "establish and improve full-process security management systems on the basis of the cybersecurity classification protection system" to strengthen data security protection. In the archives field, current archives information system classification protection is also regulated under the Cybersecurity Law and its related standards and guidelines. The Archives Information System Security Classification Protection Guidelines referenced the Information Security Technology—Basic Requirements for Classified Protection of Information Systems (GB/T 22239-2008) and Information Security Technology—Classification Guide for Classified Protection of Information Systems (GB/T 22240-2008), which have been replaced by Information Security Technology—Basic Requirements for Classified Protection of Cybersecurity (GB/T 22239-2019) and Information Security Technology—Classification Guide for Classified Protection of Cybersecurity (GB/T 22240-2020) following the enactment of the Cybersecurity Law. The two new standards changed the terminology from "information system security classification protection" to "cybersecurity classification protection," supplementing, refining, and improving the classification objects, processes, methods, and protection work content. However, the archival community has not yet revised the Archives Information System Security Classification Protection Guidelines based on the new standards, making it difficult to adapt to new technical backgrounds and legal requirements for archives information system security classification protection.

From the content-level protection perspective, the Data Security Law designates the state as the main body for establishing the data classification and tiered protection system, providing a basis for top-down state supervision. Simultaneously, it delegates the authority to formulate more granular specific catalogs of important data and specific classification and protection systems to industry authorities and regional state organs, coordinated by the national data security

work coordination mechanism, fully balancing the universality and flexibility of legal provisions. The Archives Law's determination of the scope of "archives with preservation value" and the formulation of classification standards and management methods for "permanently preserved archives" are carried out top-down by the National Archives Administration, lacking the flexibility of the Data Security Law. Meanwhile, since data and archives are at different business stages, data classification is more based on consequential criteria such as the degree of harm to national security, public interests, or legitimate rights and interests of individuals and organizations, aiming to prevent illegal acquisition, utilization, tampering, and leakage of data to protect the legitimate rights and interests of the state, public, and organizations during current data development and utilization. Archives classification aims to determine different retention periods and classification levels through appraisal of archives value, focusing on managing "historical records" to ensure their long-term preservation security. This may result in data of important value in current economic and social development (such as network information system defects, vulnerabilities, preventive measures, crowd navigation locations, large equipment target locations, and movement data) not being preserved as archives with long-term preservation value for the state and society.

3.3 Unclear Rules on Cross-Border Flow of Archives and Data As shown in Table 3 , both laws provide only general descriptions of cross-border flow of data and archives, with unclear regulatory subjects. Questions such as whether archival departments can participate in managing the cross-border flow of "important data" and whether archives exit approval requires collaborative consultation with data management departments urgently need resolution.

Although Article 31 of the Data Security Law connects with the Cybersecurity Law, stipulating that operators of critical information infrastructure should apply the Cybersecurity Law's provisions for outbound security management of important data collected and generated within China, the outbound security management methods for important data collected and generated by other data processors await further clarification. Currently, relevant specific provisions related to important data outbound flow, such as the Measures for Security Assessment of Personal Information and Important Data Outbound (Draft for Comments) and Information Security Technology—Guidelines for Security Assessment of Data Outbound (Draft), remain in draft form and have not provided specific regulations on risk prevention and control issues in cross-border flow of archives/data involving personal information and important data, nor on specific levels or categories for participation in international rules and standards for data security, limiting their reference value.

The Archives Law mainly regulates the exit approval of state-owned archives and archives stipulated in Article 22 and their duplicates. Archives security risks arising from archives exit are reflected in archives transmission, storage, and application. The Archives Law extends the forms of archives exit to include

transport, mailing, physical carriage, and internet transmission [22], covering both physical archives exit and internet transmission of archival data. However, these provisions remain general descriptions. Previous regulations based on the old Archives Law, such as the Implementation Measures of the Archives Law of the People's Republic of China and the 2015 Service Guide for Approval of Carrying, Transporting, and Mailing National Second-Level Archives and Their Duplicates Abroad [23], focused on physical archives exit and have not been adjusted according to new data transmission methods and carrier types. This may lead to low review efficiency, improper administrative approval, and buck-passing due to unclear regulatory and approval subjects, review forms, standards, and procedures for archives exit [13]. Therefore, it is urgent to supplement and improve provisions on archives exit in supporting laws and regulations such as the Implementation Measures of the Archives Law by referencing relevant legislation including the Data Security Law and Cybersecurity Law.

---

4. Foreign Experience in Coordinating the Data Security Law and the Archives Law

Faced with the rapid development of information technology and the internet in the digital age, the massive generation of electronic data, information, and documents has brought new challenges to archives management practice. The endogenous connection between data and archives is gradually reflected in foreign legislative practices related to archives and data, providing references for coordinating the development of China's Data Security Law and Archives Law.

4.1 The Global Practice of Dichotomizing Data Security into "Cybersecurity" and "Personal Data Protection" Current global data protection legislation mostly dichotomizes data security into cybersecurity and personal data security based on "fundamental data rights." In 2018, the EU implemented the General Data Protection Regulation (GDPR), focusing on personal data protection and making detailed and strict provisions on data processing principles, rights of personal data subjects, responsibilities of data processors and controllers, data supervision, cross-border data transmission, and legal liability. Countries including the United Kingdom, Germany, Egypt, and India have generally followed the GDPR's approach to personal data protection. On April 17, 2019, the European Parliament and Council promulgated the Cybersecurity Act (Regulation (EU) 2019/881) [24], imposing requirements on the security of information and communication technology products, services, and processes, placing important data security within the cybersecurity legislative framework, particularly for critical information infrastructure.

At the federal level, the United States has no unified basic data protection law but adopts sector-specific legislation for healthcare, finance, education, etc. [25], with states also working to formulate their own data protection regulations. Federally, laws such as the Cybersecurity Information Sharing Act, Federal In-

formation Security Management Act, CAN-SPAM Act, and Computer Security Act indirectly protect data security in network systems. On July 21, 2021, the Uniform Law Commission passed the Uniform Personal Data Protection Act (UPDPA) to unify state privacy legislation, though it has not yet been adopted by state legislatures and thus lacks legal effect.

Notably, although the dichotomous legislative model for data security does not directly connect with archives legislation, it can supplement archives legislation in areas such as management system security and personal information protection. For example, the United Kingdom's Data Protection Act 2018, revised and enacted in 2018, comprehensively protects citizens' personal information, 弥补了 deficiencies in personal information protection in the Public Records Act, Environmental Information Regulations, and Freedom of Information Act, becoming an important component of the UK's national archival information legal system [27]. The U.S. Freedom of Information Act stipulates standards for information disclosure and non-disclosure, granting the public the right to request archival materials from the federal government. The Privacy Act attempts to resolve contradictions between federal agencies' government information disclosure and personal information protection, requiring permission from individuals for using their personal information and ensuring lawful and reasonable information use. Overall, however, coordination between data legislation and archives legislation under the dichotomous model remains insufficient.

4.2 Swiss Practice of Integrated Archives and Data Legislation In 1992, Switzerland enacted the Federal Act on Data Protection, aiming to protect the personality and fundamental rights of data subjects. Article 8 stipulates the categories of data that archive administrators can provide access to and the forms of access, while Article 21 clarifies the application of the Federal Archives Act in personal data protection [28]. The law's enactment marked that Switzerland's archival work is regulated not only by the Federal Archives Act but also by a series of laws related to archival work [29].

In 2008, the Swiss canton of Aargau promulgated the Act on Public Information, Data Protection, and Archives, which for the first time in Switzerland placed three related themes—"public information," "data protection," and "archival work"—in the same legislation [29]. One of the legislative purposes of this Act is to ensure that public institutions such as archives departments respect individual rights and fundamental freedoms when processing personal data. The three parts do not regulate their respective management activities in isolation; archivists play an important coordinating role in the connection of public information, data, and archives protection. Chapters 6 ("Procedural Provisions and Legal Remedies") and 7 ("Final and Transitional Provisions") also provide supplementary provisions for the coordination and connection of the three areas.

In the big data era, the Swiss Federal Archives uses linked data technology to perform cross-organizational integration and linking of structured data from different sources such as federal, cantonal, and municipal governments, providing

Linked Data Archival Services (LINDAS) [30]. This "linked data service" breaks the linear management process from data to archives, optimizing and improving the utilization methods and efficiency of archives and data. Switzerland's integrated legislation on archives and data not only eliminates data providers' concerns about data ownership issues and lays a legal foundation for data generation departments and archives departments to collaboratively conduct data governance and information resource development and utilization, but also incorporates archives departments into data security protection, reducing repetitive legislation and legal conflicts at the legislative level and lowering legislative costs. Simultaneously, it can effectively ensure the coordination and integration of "data protection" and "archives management" activities at the practical level, enhance the coherence of data governance, and promote data development and utilization.

4.3 Guidance from International Organizations on Coordinating Archives and Data Legislation In October 2018, the European Archive Group (EAG) issued the Guidance on Data Protection for Archives Services as a guide for archives departments to implement the GDPR. The guidance covers general principles for processing personal data, what constitutes "archiving in the public interest," rights of data subjects, categories of personal data requiring special safeguards, data security, and measures to enhance transparency and promote compliance [31], providing practical guidance for national archives, museums, libraries, and other public and private institutions preserving archives to apply the GDPR and offering direction for archives departments and staff in personal data protection.

In March 2020, the International Council on Archives (ICA) and the International Federation of Library Associations and Institutions (IFLA) jointly issued the Draft IFLA-ICA Statement on Privacy Legislation and Archiving, arguing that archives inevitably contain personal identity information and proposing suggestions on personal data protection legislation from an archival perspective. The statement aims to establish core principles for libraries, archives, and their associations in advocating for data protection laws [32]. Evidently, international organizations' focus on archives departments' participation in data security protection also concentrates primarily on personal data.

---

5. Strategies for Coordinating the Data Security Law and the Archives Law

Addressing the internal logic, current dilemmas, and new requirements for archives and data security governance in the big data era, this study proposes recommendations for improving supporting laws and regulations of the Data Security Law and the Archives Law from the perspective of coordinating data lifecycle management laws and establishing collaborative data security mechanisms.

5.1 Clarifying Archives Departments' Participation in Data Security Collaboration Mechanisms Multiple provisions in the Data Security Law (Articles 5, 6, 9, 17, and 18) propose establishing a data security work coordination mechanism, promoting participation of relevant departments in data security protection work, and conducting collaboration in data security risk assessment, prevention, and response. Considering the overlapping management objects of data management and archives management and the intersecting functions of archives departments and data management departments, the coordination and optimization of functions between archives and data management departments should be promoted [8], integrating archives departments into the collaborative data security governance system and granting them identity in data management to provide suggestions and voice concerns from the perspective of back-end data management in data development and utilization and data security standard system construction.

Specifically, archives departments' positions in data security collaboration mechanisms should be clarified based on the Data Security Law and Personal Information Protection Law. The functional relationships among archives departments, data management departments, document management departments, government information disclosure authorities, and confidentiality administration departments should be considered holistically, with the National Archives Administration added as a member unit of the Inter-Ministerial Joint Meeting for Promoting Big Data Development. At national, local, and institutional levels, archives departments should be promoted to join collaborative data governance organizations, implementing archives participation in data security collaborative governance systems. On the other hand, based on the organizational structure of the National Inter-Ministerial Joint Conference on Electronic Records Management, data management departments should be promoted to participate in collaborative governance mechanisms for electronic archives to adapt to archives informatization and the Archives Law's management requirements for electronic archives. This would achieve two-way cooperation between archives departments and other data management departments, promoting archives departments' participation in data security collaborative governance in the big data era while also advancing archives management on the track of rule of law through joint efforts with other data management departments.

Furthermore, Article 17 of the Data Security Law proposes that "the state promotes the construction of data development and utilization technology and data security standard systems. The State Council's standardization administration department and relevant departments shall, according to their respective responsibilities, organize the formulation and timely revision of standards related to data development and utilization technology, products, and data security…" Archives departments can actively participate in this process, providing suggestions from the perspective of long-term preservation and effective utilization of data, while promoting timely updates of relevant normative documents such as the Archives Security Risk Assessment Indicator System, Basic Requirements for Archives Information System Security Protection, and Security Management

Specifications for Archives Digitization Outsourcing.

5.2 Establishing Classification Standards for Data and Archives Consistent with China's Practice On one hand, the organic connection between "data" and "archives" determines that some important data will eventually enter archives. The long-term preservation and security of "important data" can lay a quality foundation for front-end control of "important data" archiving management. The current lack of coordination between data classification and archives classification and the disconnect between data value appraisal standards and archives value appraisal standards can easily cause some data to fall into a "gray area" (i.e., data considered by archives departments as having long-term preservation value for the state and society are not classified as "important data" for protection; "important data" classified by data management departments are not preserved as archives), resulting in insufficient authenticity, integrity, availability, and security of this data. Some scholars have proposed, from the perspective of data as a governance resource, establishing data classification catalogs and important data catalogs, and building corresponding data protection catalogs and systems based on national, departmental, and industry important data catalogs to match regulatory requirements of the data classification and tiered protection system [34]. Therefore, subsequent supporting laws and regulations of the Data Security Law should include archives departments as subjects in determining "data classification" and "important data catalogs," promoting archives departments' participation in formulating subsequent laws and regulations on important data classification and outbound management.

On the other hand, archives departments should jointly discuss archives classification protection mechanisms with data management departments and relevant industry organizations to establish archives classification standards consistent with China's basic national conditions and archives management practice. Previous research has examined how to conduct archives cybersecurity classification protection work under China's cybersecurity classification protection 2.0 system requirements against the backdrop of the Cybersecurity Law elevating classification protection to the legal level [35]. The 14th Five-Year Plan for National Archives Development proposes improving archives regulations and standard systems, completing the formulation, revision, abolition, and interpretation of supporting regulations, rules, and normative documents for the newly revised Archives Law, and timely revising and cleaning up regulations, rules, and normative documents that do not meet practical needs. Therefore, the formulation of subsequent subordinate laws such as the Implementation Measures of the Archives Law should connect and coordinate with the Archives Law, Data Security Law, Cybersecurity Law, Information Security Classification Protection Management Measures, Basic Requirements for Information Security Technology and Information System Security Classification Protection, and Industrial Data Classification and Tiered Protection Guidelines (Trial) and other guiding documents and industry standards. This should be based not only on preservation needs and management dilemmas in respective fields but also on the

coherence of secure preservation and effective utilization of digital information. Specifically, archives can be divided into different security levels based on their importance, confidentiality, sensitivity, and practical utilization needs, combined with actual management requirements, to implement targeted, multi-level security protection for archives [12]. Meanwhile, archives information system classification protection standards should be updated in a timely manner according to new guidelines and standards for cybersecurity classification protection.

5.3 Improving Legal Regulations on Cross-Border Flow of Data and Archives In the era of booming digital economy, cross-border data flow has become the new normal [36]. China's Big Data Industry Development Plan (2016-2020) clearly proposes to "promote the establishment of a legal system and management mechanism for cross-border data flow, and strengthen management of important and sensitive cross-border data flow." Article 11 of the Data Security Law proposes the basic principle for cross-border data flow—secure and free flow—making "free data flow" the fundamental principle and "secure data flow" the restrictive principle to balance the dual goals of opening up and national security, providing a prudent, inclusive, and cooperation-encouraging Chinese solution for global data governance [37]. Examination of data security in cross-border flow statically reflects protection of data's original form and rights, while dynamically reflecting the legality, credibility, and controllability of the flow process [38]. Although Articles 25, 30, and 36 of the Data Security Law provide legal regulations on data export control, outbound security management of important data, and providing data to foreign judicial or law enforcement agencies, cross-border data flow still faces difficulties and challenges such as incomplete data classification systems and lack of flexible regulatory means [39].

On one hand, the Data Security Law lacks specific classification standards and legal liability clauses. On the other hand, as previously mentioned, the lack of coordination between data classification and archives classification can easily lead to unclear regulatory subjects for some data. Therefore, subsequent supporting laws and regulations of the Data Security Law should coordinate with the Archives Law, ensuring the integrity, confidentiality, availability, and security of data in cross-border flow based on archives departments' participation in determining important data and data classification standards.

Currently, the Archives Law mainly regulates the exit approval of state-owned archives and archives stipulated in Article 22 and their duplicates. Archives security risks arising from archives exit are reflected in archives transmission, storage, and application. Although the Archives Law extends the forms of archives exit to include transport, mailing, physical carriage, and internet transmission [22], covering both physical archives exit and internet transmission of archival data, these provisions remain general descriptions. Therefore, archives departments can actively participate in formulating management measures for outbound important data in accordance with Article 31 of the Data Security

Law. Subsequent formulation of archives regulations such as the Implementation Measures of the Archives Law also needs to coordinate with the Data Security Law regarding important archives catalogs, restricted lists of outbound archives, archives exit approval procedures, regulatory subjects for outbound archives, and penalties for illegal exit. When archives exit, strict review procedures should be followed, approval procedures should be handled, and data security assessment, content review, data desensitization, and establishment of archives exit records should be conducted. After archives exit, it is necessary to be familiar with and strictly comply with archives laws and regulations in the destination country or region [40], such as Russia's requirements for "local mandatory storage" [41], while also referencing Articles 2 and 26 of the Data Security Law on extraterritorial application and counter-sanctions measures to enhance the extraterritorial applicability of the Archives Law. Overall, cross-border archives flow involves not only archives exit but also archives entry. The formulation of subsequent subordinate laws of China's Archives Law should not only coordinate with relevant data legislation such as the Data Security Law, Cybersecurity Law, and Personal Information Protection Law but also analyze and understand problems in international standards and norms for cross-border data flow (such as the U.S. CLOUD Act, EU GDPR, and OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), actively participate in the formulation of international standard rules and conventions for cross-border archives flow, and thereby safeguard China's data sovereignty.

5.4 Improving Personal Privacy Protection in Both Laws On August 20, 2021, the 30th meeting of the Standing Committee of the 13th National People's Congress passed the Personal Information Protection Law, providing legal regulations for personal information processing activities. Currently, China's Data Security Law and Archives Law list personal information, personal privacy, and trade secrets together, with overlapping and intersecting conceptual scopes that increase the difficulty of distinguishing between the two concepts in legal application. Subsequent archives legislation needs to coordinate with the Civil Code of the People's Republic of China and the Personal Information Protection Law to clarify the boundaries between personal information protection and personal privacy protection.

For regulating data processing activities, on one hand, subsequent supporting laws and regulations of the Data Security Law must clarify applicable laws when data processing activities harm personal legitimate rights and interests to coordinate with the Civil Code, Tort Liability Law, Cybersecurity Law, Personal Information Protection Law, Archives Law, and other laws and regulations, constructing an overall privacy protection legal environment. On the other hand, drawing on the Aargau canton's Act on Public Information, Data Protection, and Archives, subsequent supporting laws and regulations of the Data Security Law should add risk control measures and remedy clauses for unauthorized access, use, disclosure, destruction, modification, or destruction of personal data, establishing prevention, monitoring, and remedy mechanisms for personal pri-

vacy infringement in the big data era to supplement personal privacy protection legislation in cyberspace.

For archives management activities, subsequent revisions of subordinate laws such as the Implementation Measures of the Archives Law can learn from foreign personal data protection legislation experience, coordinating with relevant laws and regulations including the Civil Code, Personal Information Protection Law, Data Security Law, Cybersecurity Law, and Archives Law, and supplementing content on personal privacy information protection in the Archives Law. For example, the Draft IFLA-ICA Statement on Privacy Legislation and Archiving proposes establishing access mechanisms for personal identity information in archives and improving relevant records management and archives planning, requiring library and archives workers to make professional judgments based on ethical principles and implement corresponding access restrictions [32]. Additionally, drawing on the Privacy Governance Framework launched by the New South Wales Information and Privacy Commission in Australia [42], collaborative tools such as personal privacy data governance frameworks and privacy risk assessment for personal data outbound flow can be developed with other data management departments to address challenges to personal privacy protection from various hacker programs, network viruses, and intentional infringements during archives collection, open sharing, publication and utilization, and exit review, thereby protecting personal privacy in archives and privacy of archives users.

Both the Data Security Law and the Archives Law represent only the beginning of legislation. Strengthening overall coordination among relevant laws, old and new policies, and specific practices is the essential meaning of ensuring data security and conducting data governance. This paper conducts a two-way examination of the driving forces for coordinated development of the Data Security Law and the Archives Law, proposing that due to the current lack of coordination between the two laws, which mainly proceed from their respective management practices, some data is left unmanaged and unregulated, making long-term preservation, effective utilization, and complete security of data impossible to guarantee. It therefore points out that archives departments' participation in data governance, coordination of classification standards for data and archives, security protection in cross-border flow of data and archives, and personal privacy protection should be integrated into the formulation, revision, abolition, and interpretation of supporting regulations, rules, and normative documents for the Data Security Law and the Archives Law. Meanwhile, current controversies over the division of archives and data management functions, how archives departments can conduct collaborative data governance with data management departments, and the integration of archives management thinking and data management thinking require further in-depth research and discussion.

References

[1] 审时度势精心谋划超前布局力争主动实施国家大数据战略加快建设数字中国 [N]. People's Daily, 2017-12-10(001).

[2] Zhai Zhiyong. The Systematic Positioning of the Data Security Law[J]. Journal of Soochow University (Philosophy & Social Science Edition), 2021, 42(1): 73-83.

[3] Zhang Meng. Comparative Analysis of Provisions in the Data Security Law Draft and the Cybersecurity Law[J]. Network Security and Informatization, 2020(10): 25-26.

[4] Liu Guifeng, Ruan Bingying, Liu Qiong. Strengthening Data Security Protection and Improving Data Governance Capabilities—Interpretation of the Data Security Law of the People's Republic of China (Draft)[J]. Journal of Library and Information Science in Agriculture, 2021, 33(4): 4-13.

[5] Ma Zhongfa, Hu Ling. On the Improvement of China's Data Security Protection Legal System[J]. Science Technology and Law, 2021, (2): 1-7, 75.

[6] Xu Jiujiu. The Balancing Path of Data Rule of Law Security and Development Values—From the Perspective of Breakthroughs and Dilemmas in the Data Security Law (Draft)[J]. Journal of Shandong University of Science and Technology (Social Sciences), 2021, 23(2): 38-43, 61.

[7] Zhao Shenghui, Hu Ying. Analysis and Enlightenment of the Underlying Logic of "Archival Datafication"[J]. Archives Science Bulletin, 2021(4): 20-27.

[8] Liu Yuenan. Data Governance: A New Perspective and Function for Archives Management in the Big Data Era[J]. Archives Science Study, 2020(5): 50-57.

[9] Zhao Shenghui, Hu Ying. Possessing Holistic Memory: An Outline of Archival Domain Data Ontology Management[J]. Shanxi Archives, 2020(6): 17-27.

[10] Future Rule of Law Research Institute of Renmin University of China. Establishing and Improving the Data Security Legal System[N]. Economic Information Daily, 2020-09-15(008).

[11] Deng Lingbin. Interpretation of the Data Security Law (Draft) and Countermeasures for China's Library and Information Science Community[J]. Journal of Intelligence, 2020, 39(12): 83-87.

[12] Jin Bo, Yang Peng. Analysis of Archival Data Security Governance Strategies in the Big Data Era[J]. Information Science, 2020, 38(9): 30-35.

[13] Geng Zhijie, Liu Zhisen. Implementation Dilemmas and Improvement Strategies for Archival Data Internet Transmission Exit[J]. Zhejiang Archives, 2021(3): 24-26.

[14] Ding Jiayou, Zhou Hanxiao, Zhang Zhaoyu. Data Security and High-Quality Development of Archives—Interpretation and Reflection on the 14th Five-Year Plan for National Archives Development[J]. Archives and Construction, 2021(9): 12-15, 11.

[15] Wu Weiming, Wu Li. Comprehensive Information Security and Rational Data Utilization—Brief Review of the Data Security Law (Draft)[J]. Information Security and Communications Privacy, 2020(8): 23-28.

[16] Wang Xiezhou, Wang Lulu. Challenges to Archival Work in the "Internet Plus" Era[J]. Archives Science Study, 2016(6): 66-69.

[17] Xu Yongjun, Li Mengqiu. Reform of the Archives Management System from the Perspective of Digital Continuity Strategy[J]. Archives and Construction, 2020(5): 4-10.

[18] Qian Yi. Analysis of Problems and Strategies for Digital Archives Object Preservation in Data State Environments[J]. Archives Science Bulletin, 2019(4): 40-47.

[19] Wang Yingwei, Yang Qian. The Security Concept of the Archives Law of the People's Republic of China from the Perspective of the Overall National Security Concept[J]. Archives Science Study, 2020(6): 78-85.

[20] National Archives Administration of the People's Republic of China. Summary of Basic Information on National Archives Authorities and Archives in 2020 (Part 2)[EB/OL]. (2021-08-06)[2021-08-27]. https://www.saac.gov.cn/daj/zhdt/202108/6262a796fdc3487

[21] Chen Xingyue. The Formal Inclusion of Data Classification and Tiering in Law Has Great Practical Guiding Significance[J]. Information Security Research, 2020, 6(10): 949-952.

[22] Policy and Regulation Research Department of National Archives Administration. Interpretation of the Newly Revised Archives Law of the People's Republic of China[J]. China Archives, 2020(7): 24-25.

[23] Policy and Regulation Department of National Archives Administration. Approval for Carrying, Transporting, and Mailing National Second-Level Archives and Their Duplicates Abroad[EB/OL]. [2021-04-16]. https://www.saac.gov.cn/daj/xzsp/201509/5b499a02ce9f495baec0c8288b5abede.shtml.

[24] OFFICIAL JOURNAL OF THE EUROPEAN UNION. Regulation (EU) 2019/881 of the European parliament and of the council[EB/OL]. (2019-04-17)[2021-04-27]. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&qid=16

[25] Long Weiqui. Research on the Construction of New Data Property Rights and Its System[J]. Tribune of Political Science and Law, 2017, 35(4): 63-77.

[26] Zhang Zhen, Li Yan. Review of the U.S. "Overview of Data Protection Laws" Report[J]. Secrecy Science and Technology, 2019(8): 29-35.

[27] Cao Yu, Lai Wenyuan. Overview of the UK National Archives Legal System[J]. Journal of Liaoning University (Philosophy and Social Sciences Edition), 2011, 39(5): 79-86.

[28] THE PUBLICATION PLATFORM FOR FEDERAL LAW. Loi fédérale du 19 juin 1992 sur la protection des données (LPD)[EB/OL]. [2021-05-09]. https://www.fedlex.admin.ch/eli/cc/1993/1945_{{{1945}}_{1945}}}/fr.

[29] Policy and Regulation Research Department of National Archives Administration. Selected Compilation of Archives Laws and Regulations from Foreign Countries and Regions[M]. Beijing: China University of Political Science and Law Press, 2017.

[30] Wang Zhiyu, Wang Xiaoyu. Research and Enlightenment on the Characteristic Functions of the Swiss Federal Archives[J]. Beijing Archives, 2021(5): 40-43.

[31] EUROPEAN ARCHIVE GROUP. Guidance on data protection for archives services[EB/OL]. [2020-07-15]. https://ec.europa.eu/info/sites/info/files/eag_{{{draft}}*{{guidelines}}}1*{11}

[32] INTERNATIONAL COUNCIL ON ARCHIVES. IFLA-ICA statement on privacy legislation and archiving[EB/OL]. [2020-07-26]. https://www.ica.org/sites/default/files/privacy_{{{leg

[33] Huang Daoli, Hu Wenhua. China's Data Security Legislative Situation, Dilemmas and Countermeasures—With Comments on the Data Security Law (Draft)[J]. Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition), 2020, 33(6): 9-17.

[34] Ou Li. Upholding Party Leadership over Data and Ensuring Data Security[J]. Flag, 2021(8): 45-47.

[35] Zheng Chuan, Cao Yang, Xiang Yu, et al. Archives Cybersecurity Classification Protection Under New Situations: Changes and Countermeasures[J]. Shanxi Archives, 2021(2): 25-34.

[36] Yang Shudong, Xie Zhuojun. Exception Clauses in Trade Regulation of Cross-Border Data Flow: Positioning, Paradigms and Reflections[J/OL]. Journal of Chongqing University (Social Science Edition): 1-15[2021-08-30]. http://kns.cnki.net/kcms/detail/50.1023.C.20210826.1451.002.html.

[37] Xu Ke. Freedom and Security: The Chinese Solution for Cross-Border Data Flow[J]. Global Law Review, 2021, 43(1): 22-37.

[38] Huang Xianqing. The Construction Path of China's Cross-Border Data Flow Regulatory Rules Under the Background of Digital Trade[J]. Southwest Finance, 2021(8): 74-84.

[39] Wang Zhijie. On the Improvement of China's Cross-Border Data Flow Regulation—Based on the Perspective of Balancing Data Security and Data Openness[J]. Fujian Finance, 2021(7): 9-16.

[40] Xu Yongjun, Shu Rong, Li Mengqiu. Legal Conflicts and Applicable Principles Faced by Chinese Enterprises' Overseas Archives Management[J]. Archives Science Bulletin, 2018(4): 9-14.

[41] He Bo. Russian Cross-Border Data Flow Legislative Rules and Enforcement Practice[J]. Big Data Research, 2016, 2(6): 129-134.

[42] INFORMATION AND PRIVACY COMMISSION. Privacy governance framework[EB/OL]. [2021-04-16]. https://www.ipc.nsw.gov.au/privacy/agencies/privacy-governance-framework.

Author Contributions

Wang Yujue: Proposed the research topic, designed the paper structure, guided and revised the paper; Wu Yinuo: Collected materials, organized and wrote the paper, revised the paper; Ling Minhan: Collected materials, wrote the initial draft.

Abstract: *[Purpose/Significance]* By analyzing the respective emphasis and overlap of the Data Security Law and the Archives Law in terms of regulatory objects, legislative purposes, and legislative principles, this paper explores the necessity and possible pathways for promoting the coordinated development of the two laws to provide references for subsequent legislation on archives and data. *[Method/Process]* Through literature review and comparative analysis, this paper identifies the main problems in the coordinated advancement of the two laws and makes suggestions for formulating supporting subordinate legislation by drawing on foreign experiences. *[Result/Conclusion]* The study finds that, starting from their respective management practices, the two laws lack coordination in legal regulations concerning archives and data protection, classification standards, and cross-border flow, resulting in some data falling into a "gray area" with no guarantee of data security. The paper proposes clarifying the participation of archival departments in data governance; establishing classification standards for data and archives consistent with China's actual conditions based on the continuity of long-term data preservation; coordinating between archival and data departments to establish laws, regulations, and management mechanisms for the cross-border flow of important data; and improving personal privacy protection content in both laws.

Keywords: Data Security Law; Archives Law; data security; archives legislation; data legislation

Note: Figure translations are in progress. See original paper for figures.