WEP Warwick Evans Publishing

International Journal of Global Economics and Management

ISSN: 3005-9690 (Print), ISSN: 3005-8090 (Online) | Volume 6, Number 3, Year 2025
DOI: https://doi.org/10.62051/ijgem.v6n3.23
Journal homepage: https://ijgem.org

Research on Security Assurance Mechanisms for Government Data in the Digital Rule of Law Framework

Xincheng Song

School of Law, Anhui University of Finance & Economics, Bengbu Anhui 233030, China

ABSTRACT

This study investigates the security assurance mechanisms for government data within the digital rule-of-law framework, addressing emerging challenges in data governance under rapid technological advancement. Through systematic analysis of China's evolving data security legislation, the research identifies structural deficiencies in current administrative data protection systems, particularly in risk assessment protocols and accountability implementation. Comparative examination reveals divergent governance models from the United States' sectoral approach to the EU's comprehensive GDPR framework and the UK's post-Brexit regulatory adjustments, providing multidimensional references for institutional optimization. The proposed policy recommendations emphasize establishing dynamic risk evaluation mechanisms and strengthening multi-tiered supervision systems, while advocating for enhanced interdepartmental coordination and technological empowerment in security governance. These findings contribute to the theoretical development of digital government governance and offer practical pathways for improving data security management in public administration. The research outcomes hold significant implications for advancing legal frameworks in the digital governance era and strengthening institutional safeguards for national data sovereignty.

KEYWORDS

Digital Rule of Law; Government Data Security; Risk Assessment Mechanisms; International Comparative Analysis; Legal Framework Optimization

1. INTRODUCTION: RESEARCH BACKGROUND AND OBJECTIVES

The digital transformation of government operations has fundamentally reshaped public administration in the 21st century. As nations increasingly adopt data-driven governance models, the security of government data has emerged as a critical component in maintaining national sovereignty and public trust. This evolution stems from the dual demands of technological progress and legal system development, where data serves simultaneously as an administrative resource and a potential vulnerability.

The core of this transformation lies in China's strategic promotion of the construction of a digital law-based government(digital rule-of-law government), as outlined in the Implementation Outline for Building a Law-Based Government (2021-2025). This national initiative emphasizes creating intelligent governance systems through comprehensive data integration while mandating robust security protections. The inherent tension between data openness for administrative efficiency and data protection for national security forms the core challenge this research addresses. Government data repositories now contain sensitive information ranging from national infrastructure details to citizens' personal records, making their protection equivalent to safeguarding critical national assets.

Three primary challenges have emerged in current administrative practices. First, the rapid adoption of emerging technologies like cloud computing and big data analytics has outpaced existing regulatory frameworks, creating vulnerabilities in data lifecycle management. Second, the implementation of accountability mechanisms often lags behind legislative developments, particularly in cross-departmental data sharing scenarios. Third, traditional risk assessment models struggle to adapt to the dynamic nature of cyber threats in interconnected digital ecosystems. These challenges are compounded by the dual requirements of maintaining data utility for public services while ensuring absolute security integrity.

The research objectives are threefold: to systematically examine structural deficiencies in China's current government data protection systems, to analyze comparative international approaches for institutional optimization, and to propose actionable policy solutions. The investigation focuses specifically on improving risk assessment protocols and accountability implementation mechanisms within administrative agencies. By studying the United States' sectoral governance model, the EU's comprehensive GDPR framework, and the UK's post-Brexit regulatory adjustments, this study seeks to develop adaptive solutions that balance security requirements with operational efficiency.

This investigation holds both theoretical and practical significance. Academically, it contributes to developing digital governance theory by establishing evaluation criteria for data security mechanisms in public administration. Practically, the findings aim to assist policymakers in creating dynamic supervision systems that can evolve with technological advancements. The ultimate goal is to formulate a security assurance framework that supports China's digital government transformation while maintaining compliance with international data governance standards, thereby strengthening institutional safeguards for national data sovereignty in the digital age.

2. ANALYSIS OF CHINA'S CURRENT GOVERNMENT DATA SECURITY LEGAL FRAMEWORK

2.1. Evolution of Data Security Legislation in China

China's data security legislation has developed through three distinct phases, reflecting the nation's growing understanding of digital governance challenges. The initial foundational period (1990s-2010) established basic cyber infrastructure protections through regulations like the Computer Information System Security Protection Ordinance (1994). These early measures focused primarily on physical infrastructure protection and basic network security protocols, laying groundwork for subsequent digital governance frameworks.

The acceleration phase (2011-2016) saw comprehensive legal responses to emerging digital risks. Milestone legislation included the Cybersecurity Law (2016), which introduced critical data classification systems and cross-border data transfer controls. This period marked a strategic shift from reactive technical safeguards to proactive governance frameworks, establishing mandatory security assessments for critical information infrastructure operators.

Current developments (2017-present) demonstrate sophisticated legal adaptation to complex data ecosystems. The Data Security Law (2021) and Personal Information Protection Law (2021) created China's first comprehensive data governance framework, introducing concepts like data classification management and security accountability systems. These laws established differentiated protection requirements based on data sensitivity and economic value, while mandating regular risk assessments for government data processors.

Key legislative characteristics emerge from this evolutionary process. First, the legal framework prioritizes national security while balancing public service efficiency, requiring government agencies to implement security measures without hindering administrative functions. Second, it emphasizes dynamic adaptation, with provisions for updating technical standards alongside technological

advancements. Third, the system incorporates multi-level supervision mechanisms, combining internal audits with third-party evaluations.

Implementation challenges persist despite legislative progress. Technical specification gaps remain between broad legal principles and practical operational requirements, particularly in emerging fields like AI governance and blockchain applications. Enforcement consistency varies across administrative levels, with local governments sometimes struggling to interpret national standards for specific regional contexts. The system continues evolving through supplementary regulations, such as the 2023 guidelines for government cloud security management, demonstrating ongoing efforts to address implementation complexities.

2.2. Institutional Challenges in Government Data Security Assurance

China's government data security framework faces multiple implementation challenges despite establishing comprehensive legal foundations. Three primary institutional gaps hinder effective security assurance in administrative operations. First, risk assessment mechanisms lack dynamic adaptability to evolving cyber threats. Current protocols primarily employ periodic evaluations that cannot adequately address real-time vulnerabilities in interconnected data systems. This static approach creates security blind spots, particularly when government agencies adopt emerging technologies like cloud computing and IoT devices without corresponding updates to risk evaluation criteria.

Second, accountability implementation suffers from fragmented enforcement across administrative levels. While national legislation mandates strict security responsibilities, local governments often struggle with operational interpretation due to varying technical capacities and resource allocations. A notable example appears in cross-departmental data sharing scenarios, where unclear liability boundaries frequently lead to responsibility shifting between data providers and users. This enforcement inconsistency undermines the effectiveness of security accountability systems established by recent laws like the Data Security Law.

Third, technical standardization lags behind technological adoption in public administration. Many government entities utilize advanced data processing tools without unified security specifications, resulting in incompatible protection measures across different systems. The absence of mandatory encryption standards for sensitive data transfers between agencies exemplifies this challenge. Moreover, legacy systems in some local governments remain incompatible with modern security requirements, creating weak points in national data protection networks.

The legal framework's coordination mechanisms reveal structural deficiencies in three aspects. Sector-specific regulations occasionally conflict with general data security laws, causing implementation ambiguities for agencies handling multiple data types. For instance, healthcare administration departments face overlapping compliance requirements from medical data regulations and broader cybersecurity mandates. Additionally, the lack of integrated supervision systems allows gaps between internal audits and third-party assessments, particularly in verifying compliance with data minimization principles. Finally, public-private partnership projects encounter undefined security responsibility divisions when outsourcing data processing to technology companies.

Personnel capability constraints further exacerbate these institutional challenges. Many government IT departments lack specialists proficient in both legal compliance and advanced security technologies, leading to inadequate implementation of mandated protection measures. Training programs often emphasize theoretical knowledge over practical skills for threat detection and incident response, leaving frontline operators unprepared for sophisticated cyberattacks. This human resource gap persists despite increased budgetary allocations for digital infrastructure, reflecting systemic issues in technical talent cultivation within public sector organizations.

3. INTERNATIONAL EXPERIENCES IN GOVERNMENT DATA SECURITY GOVERNANCE

3.1. Comparative Analysis of U.S. Federal Data Protection Frameworks

The United States employs a sector-specific approach to federal data protection, characterized by decentralized legislation tailored to distinct industry requirements. This framework operates through three primary mechanisms: vertical industry regulations, cross-cutting technical standards, and cooperative federal-state enforcement. Unlike comprehensive data protection regimes, the U.S. system develops specialized rules for sensitive sectors while maintaining baseline security requirements through non-regulatory guidance.

Healthcare and education sectors exemplify this sectoral model. The Health Insurance Portability and Accountability Act (HIPAA) mandates strict security controls for protected health information, requiring covered entities to implement access controls and encryption protocols. Similarly, the Family Educational Rights and Privacy Act (FERPA) establishes specific protections for student records, prohibiting unauthorized disclosures without consent. These laws coexist with horizontal frameworks like the Federal Information Security Modernization Act (FISMA), which sets general security requirements for federal agencies' information systems.

Three distinctive features define the U.S. approach. First, regulatory granularity allows precise adaptation to sector-specific risks - financial institutions under Gramm-Leach-Bliley Act face different compliance obligations than energy providers regulated by the North American Electric Reliability Corporation standards. Second, technical specifications primarily emerge through National Institute of Standards and Technology (NIST) guidelines rather than legislative mandates, enabling rapid updates to address evolving cyber threats. Third, enforcement responsibilities are distributed across multiple agencies, with the Federal Trade Commission handling consumer data violations while sector-specific regulators oversee industry compliance.

The system demonstrates notable strengths in operational flexibility and technological responsiveness. Sectoral regulations effectively address unique risk profiles in critical industries, while NIST's framework provides adaptable security controls applicable across government systems. Public-private partnerships facilitate information sharing about emerging threats through initiatives like the Cybersecurity and Infrastructure Security Agency's (CISA) joint advisories.

However, structural limitations emerge in three aspects. The fragmented legal landscape creates compliance complexities for entities handling multiple data types, as seen in hospitals managing both health records and payment information. Decentralized enforcement occasionally leads to inconsistent penalty applications across sectors. Moreover, reliance on voluntary standards adoption results in uneven implementation, particularly among smaller government contractors lacking technical resources.

For China's digital governance context, the U.S. experience offers cautionary insights and partial solutions. The sectoral model's emphasis on risk-adapted controls aligns with China's need for differentiated protection levels in government data systems. NIST's technology-neutral standards provide a reference for developing dynamic technical specifications that accommodate emerging technologies like AI-driven analytics. However, the U.S. system's lack of centralized oversight contrasts with China's integrated administrative structure, suggesting hybrid models that combine unified principles with sector-specific implementation guidelines could prove more effective. Key transferable elements include mechanisms for regular security control updates and cross-sector threat intelligence sharing, which could enhance China's existing risk assessment frameworks without compromising centralized governance advantages.

3.2. EU GDPR and UK Post-Brexit Data Governance Models

The European Union's General Data Protection Regulation (GDPR) represents a landmark in comprehensive data governance, establishing rigorous standards for personal information protection across member states. Implemented in 2018, this framework mandates strict requirements for data controllers and processors, including mandatory breach notifications within 72 hours and substantial fines for non-compliance. Its "privacy by design" principle requires integrating data protection measures into all stages of system development, particularly relevant for government agencies handling citizen information. Three core mechanisms define GDPR's operational effectiveness: data minimization requirements limiting collection to necessary information, storage limitation provisions enforcing periodic data purging, and cross-border transfer restrictions through adequacy decisions for third countries.

Post-Brexit Britain's data governance model demonstrates adaptive regulatory evolution while maintaining GDPR's foundational principles. The UK retained the core of GDPR through its "UK GDPR" framework but introduced modifications enhancing regulatory flexibility. The Information Commissioner's Office (ICO) gained expanded authority to develop sector-specific guidance, particularly for government data sharing initiatives. A notable innovation involves the creation of "data adequacy partnerships" with non-EU countries, enabling customized international data flows while maintaining protection standards. This dual approach preserves seamless data exchange with EU nations under adequacy decisions while pursuing independent digital trade agreements.

Comparative analysis reveals distinct operational characteristics between the two models. The EU maintains centralized enforcement through the European Data Protection Board, ensuring uniform interpretation across member states. In contrast, the UK's system emphasizes regulatory agility through periodic reviews of adequacy decisions and faster adaptation to emerging technologies. Both systems share strong accountability mechanisms requiring documented compliance measures, but the UK model introduces simplified procedures for low-risk government data processing activities.

Key lessons emerge for enhancing data security governance. GDPR's risk-based approach to data protection impact assessments offers a replicable framework for identifying vulnerabilities in government data systems. The UK's experience illustrates how maintaining core principles while allowing regulatory flexibility can facilitate both international cooperation and domestic innovation. The adequacy decision mechanism provides a reference for establishing secure cross-border government data sharing protocols without compromising sovereignty.

Practical applications for China's context include adopting GDPR-style accountability tools to strengthen oversight of third-party data processors in public-private partnerships. The UK's sector-specific guidance development process suggests methods for tailoring general data protection principles to different government functions. Both models emphasize the importance of independent supervisory authorities, reinforcing the need for enhancing technical capabilities within China's regulatory bodies. The integration of continuous compliance monitoring in GDPR aligns with requirements for dynamic risk assessment mechanisms in China's evolving digital governance landscape.

4. POLICY RECOMMENDATIONS AND CONCLUDING REMARKS

To strengthen government data security within China's digital rule-of-law framework, this study proposes three actionable policy recommendations supported by international best practices and domestic implementation requirements. These measures aim to address identified institutional gaps while maintaining administrative efficiency and technological adaptability.

First, establishing dynamic risk assessment mechanisms proves essential for modern data governance. Traditional periodic evaluations should evolve into continuous monitoring systems integrating real-

time threat detection and predictive analytics. Drawing from the EU GDPR's data protection impact assessment model, government agencies could implement automated risk scoring tools that update security protocols based on evolving cyber threats. This approach aligns with the Central Committee's emphasis on "precise governance through technological empowerment" in the 2021-2025 Outline for the establishment of a rule of law government. Practical implementation would involve developing standardized risk indicators for different data types and administrative scenarios, supported by shared threat intelligence platforms across departments.

Second, enhancing multi-tiered supervision systems requires structural reforms in accountability implementation. The UK's post-Brexit regulatory adjustments demonstrate how centralized principles can coexist with flexible enforcement. China's system could benefit from creating specialized data security oversight positions within each administrative unit, directly accountable to higher-level supervisory bodies. These roles would bridge the gap between national legislation and local implementation, ensuring consistent application of security standards across provincial and municipal governments. Complementing this, third-party audit mechanisms similar to GDPR compliance certifications could be mandated for critical data systems, creating additional accountability checkpoints.

Third, optimizing interdepartmental coordination mechanisms addresses systemic vulnerabilities in cross-agency data sharing. The U.S. sectoral approach highlights the value of specialized protocols for different data types, which China could adapt through customized data sharing agreements between departments. Establishing clear responsibility matrices for joint data projects would prevent accountability gaps, while standardized API interfaces could ensure technical compatibility between different security systems. This aligns with the public data sharing principles outlined in recent guidelines from the National Data Administration, particularly regarding unified authentication protocols and access permission management.

Technological empowerment forms the cornerstone of these reforms. Implementing blockchain-based audit trails for sensitive data transactions would enhance traceability, while AI-driven anomaly detection systems could significantly improve threat response times. These technical measures should be paired with mandatory cybersecurity training programs for government personnel, focusing on practical skills for identifying phishing attempts and securing cloud-based systems.

The proposed framework balances security requirements with governance efficiency through three strategic integrations: merging legal compliance with technical safeguards, connecting centralized oversight with localized implementation, and aligning data protection with service optimization goals. This approach addresses the core challenge of maintaining data utility while ensuring security, as emphasized the digital construction of a law-based government.These recommendations contribute to both theoretical and practical dimensions of digital governance. Academically, they expand the conceptual understanding of adaptive security mechanisms in public administration. Practically, they provide executable solutions for improving China's data security posture while supporting ongoing digital government transformation. The proposed measures ultimately strengthen institutional safeguards for national data sovereignty, ensuring secure and sustainable development of China's digital governance ecosystem in alignment with global best practices.

ACKNOWLEDGEMENTS

This work is supported by Anhui University of Finance & Economics 2025 Undergraduate Research innovation fund project fund, Project number: XSKY25047ZD.

REFERENCES

[1] Dang Min. Exploration of the Path to the Legalization of Government Data Openness from the Perspective of Digital Government [J]. Journal of Suihua University, No. 2,2025, 35-37.

[2] Su Li. Administrative Law Guarantee for the Construction of Digital Government in China [J]. Hebei Legal Vocational Education, No. 1,2024, 86-94.

[3] Xiaohan Yuan. Application of Data Governance Models in the Context of the Digital Economy [J]. Proceedings of Business "and Economic Studies", Issue 4, 2024, 172-176.

[4] S.Prince Chelladurai. Intelligent Digital Envelope for Distributed Cloud-Based Big Data Security [J]. Computer Systems "Science & Engineering", Issue 7,2023, 951-960.

[5] Li Yanhua Digital Development Rights in Developing Countries: Where the Governance Rules for Cross-Border Data Flows [J]. The Journal of Human Rights, Issue 5, 2023, 1040-1066.