Research on Technical Security Vulnerabilities and Legal Regulations in the Storage Link of Personal Information Protection: Based on the Analysis of Classic Data Leakage Incidents

Junyu Lai
Guangzhou College of Commerce, Guangzhou, Guangdong, China

Abstract: With the development of the digital economy, personal information has become an important strategic resource. There is a significant "technology-legal gap" between the frequent technical security breaches in the storage section of personal information protection and the lagging legal regulations, leading to an escalation of the risk of large-scale data breaches. Based on an analysis of classic data breaches, this paper systematically reveals the predicaments and root causes caused by this gap. The core of the study is to propose and demonstrate a dynamic compliance framework of "legalization of technical standards + strengthening of liability" : through the two-way interaction of mandatory technical certification systems and stepped punitive damages mechanisms, to drive the transformation of personal information leakage towards proactive prevention. The framework aims to systematically bridge the gap between technical security and legal regulation, providing a critical path for improving the supporting mechanisms for the implementation of the Personal Information Protection Law.

Keywords: Technical Security Vulnerabilities; Data Breach Cases; Storage Section; Legal Regulation

1. The Dilemma and Risk of the "Technology-Law Gap" in Storage: Based on Classic Event Analysis

1.1 Analysis of Technical Security Vulnerabilities in Classic Data Breaches

1.1.1 Configuration oversight vulnerability: 360 leak (2010)

In December 2010, a server used by 360 to store cloud security query logs was wrongly configured with permissions, which led to sensitive data such as user access records and URL transmission account information being crawled by Google search engine, involving more than 300 million users. The root cause of the incident was that the server did not turn off the default indexing function and did not desensitize the log data-a "low-level configuration error" that is highly representative in distributed cloud architectures. As Tai Xiaoning (2025) pointed out in his research on vulnerability scanning technology, "configuration omissions in the cloud era (such as opening default ports and over-granting permissions) have become the most frequent vulnerabilities, accounting for more than 45%." 360 later defended itself with "general security software technology", but exposed the enterprise's cognitive bias regarding storage security: equating data upload with security protection and neglecting permission control and data isolation in the storage process [3].

1.1.2 API authentication missing vulnerability: Lenovo/Iomega NAS leak (2018)

Security researchers discovered via the Shodan platform that the NAS devices of the Lenovo EMC joint venture had 36TB of data (including configuration information of 5,114 devices, 20,000 financial documents, 405,000 images) exposed to the public network due to the lack of an authentication mechanism in the API interface. Attackers could list and download files simply by sending a request, which was like "opening an unlocked warehouse." Zhao et al. (2025) emphasized in their research on data encryption storage that "API, as the core channel for data interaction, the absence of its authentication mechanism will directly break through the storage security defense line", and the fact that the firmware development in this incident did not incorporate API permission control into the security baseline precisely

reflects the absence of security responsibility in the enterprise technical design stage.

1.1.3 System management flaws and vulnerabilities: Amazon S3 bucket leak (2019)

UpGuard and DataBreaches.net research teams discovered at the same time that misconfigured Amazon S3 buckets from two enterprises leaked more than 300,000 medical records belonging to Medico. The core of the vulnerability was that the buckets did not have the "private access" setting enabled and access log auditing was not enabled-a flaw clearly defined in Chen Jing's (2025) big data security research as a "managerial vulnerability", that is, "enterprises overly rely on the security promises of cloud service providers, ignore their own management responsibilities for storage assets, and ultimately create a 'cloud security vacuum'" [4]. It is notable that Amazon provided complete security configuration tools at the time. The key to the incident was that the enterprise failed to implement basic security operations, highlighting the disconnect between the availability of technical tools and the enterprise's management capabilities.

1.2 The Weakness and Lag of Current Legal Regulations in Addressing Storage Vulnerabilities

The above cases all confirm the three major shortcomings of legal regulation:

1.2.1 The absence of technical standards leads to "compliance without evidence"

Between 2010 and 2019, China did not have a specific technical standard for personal information storage. The Cybersecurity Law (2017) only requires in principle "necessary technical measures", without specifying details such as permission control and encryption standards in the storage process. In the case of Amazon S3, enterprises were unable to determine whether "private access settings" were "necessary measures", resulting in compliance actions being merely formalities. Xu Huaqing (2025) pointed out, "The principle-based provisions of the law leave enterprises in a dilemma of 'not knowing how to comply' and also leave ambiguity for regulatory enforcement." [10]

1.2.2 Ambiguous responsibility determination leads to "no way to hold people accountable"

The Lenovo NAS incident involves multiple entities, including the device manufacturer (Lenovo), the joint venture (LenovoEMC), and the cloud service provider. The current law does not clearly define the boundaries of liability for storage vulnerabilities. Ren Yanjun (2025) mentioned in his research on data crimes that "at that time, the criminal law only regulated data theft through the crime of 'illegally obtaining data from computer information systems', but did not establish a specific crime for the responsible subjects of storage vulnerabilities", and ultimately the incident ended with the enterprise privately fixing the vulnerability, with no subject bearing legal responsibility [15].

1.2.3 Cross-border regulatory void leads to "ineffective relief"

In the Amazon S3 incident, medical data was stored on servers outside China, and our regulatory authorities were unable to conduct investigations due to jurisdiction limitations, making it difficult for victims to claim compensation through judicial means. Zhao Ruhan (2025) found in the comparison of governance among China, the United States and Europe that "China lacked a regulatory collaboration mechanism for cross-border data storage at that time and often fell into the predicament of 'not being able to control and not being able to catch up' when facing cross-border data leakage", in sharp contrast to the "long-arm jurisdiction" of the EU GDPR [1].

1.3 The Formation of the "Technology-Legal Gap" and the Mechanism of Risk Superposition

The essence of the fault is the contradiction between the "fast iteration" of technology and the "slow adaptation" of the law, and its risk transmission presents three layers of superposition:

1.3.1 The first layer: from the native risk of technology to a single leak incident

The distributed nature of the cloud architecture, such as multi-node backups and cross-regional storage, makes the vulnerability attack surface expand exponentially [13]. As in the 360 incident, a single server vulnerability spread across the entire network through cloud synchronization, escalating the scale of the data breach from "local" to "global". Tan Xin (2025) pointed out in his research on AI security that "the prevalence of automated scanning tools has compressed vulnerability exploitation time from 'days' to 'hours', and the speed at which technical risks erupt far exceeds legal response capabilities." [5]

1.3.2 The second layer: From legal lag to risk transmission amplification

The failure of deterrence leads to insufficient corporate security investment: Before the Data Security Law was introduced in 2019, the maximum fine for data breaches was only 500,000 yuan, far lower than the cost of corporate security investment (more than one million yuan per year) [6]. Yan Qi (2025) found in his research on data crimes that "at that time, 83% of small and medium-sized enterprises had the perception that 'security investment was not worthwhile' and chose to cut storage security budgets", creating a vicious cycle of "retained vulnerabilities-frequent leaks" [9].

1.3.3 The third layer: From risk accumulation to systemic social risk

In 2018–2019, there were 12 consecutive storage breaches in the e-commerce and healthcare sectors, which led to a 37% drop in public trust in the digital economy (China Cybersecurity Report 2020). The "bad money drives out good" effect emerges: if a healthcare company's cost increases by 15% due to implementing storage encryption, and unimplemented competitors seize the market with low prices, it eventually leads to a decline in security across the entire industry [14].

2. A Deep Examination of the Nature of Technical Vulnerabilities and the Root of Legal Weaknesses

2.1 Systematic Attribution of Technical Security Vulnerabilities

Storage vulnerabilities are not isolated technical issues, but rather the result of interweaving four systemic factors:

2.1.1 The inherent complexity of the technical architecture

The "microservice splitting" of cloud-native architecture involves dozens of components in the storage system (such as containers, API gateways, and distributed databases), and any vulnerability in any component can trigger a chain reaction. As in the Lenovo NAS incident, the API interface vulnerability originated from compatibility flaws between the firmware and the database, and the complex technology stack took more than 72 hours to troubleshoot. Gao Yang's (2025) research on AI protection points out that "modern storage systems have more than ten million lines of code, and human auditing is difficult to cover all vulnerabilities, and AI detection technology must be relied upon." [8]

2.1.2 Security imbalances driven by economy

The "fast fish eat slow fish" market logic has led businesses to prioritize storage efficiency over security design. In the case of the Amazon S3 incident, Medico shut down the "secondary authentication" feature to shorten data upload time-a choice that served short-term economic benefits but violated security principles. The data encryption research by You Pengcheng (2025) shows that "enabling storage encryption reduces data access speed by 20%, and most enterprises choose to sacrifice security for user experience." [7]

2.1.3 Structural flaws in organizational management

The absence of a DevSecOps culture leads to a disconnect between development and security: An investigation after the 360 incident found that the configuration of its storage servers was independently handled by the development team without being reviewed by the security team. Chen Kunling (2025) 's "AI + Security" study points out that "only 17% of enterprises embed security audits into the storage system development process, resulting in vulnerabilities being discovered only after going live, and the cost of fixing increases tenfold." [11]

2.1.4 The industrialization of attack ecosystems has matured

The division of labor in the black industry chain (such as vulnerability mining-tool development-data trafficking) lowers the threshold for attacks. In 2019, in dark web data transactions, storage vulnerability exploitation tools cost only 500 yuan, while a piece of personal information costs 0.5 yuan. "Low investment, high return" has spurred rampant attacks. Ren Hong (2024) 's research on smart contract security points out that "the 'plug and play' of attack tools enables non-professional hackers to launch storage attacks, and the generalization speed of technical risks is far faster than expected."

2.2 Institutional Root Causes of Legal Regulatory Shortcomings

The core of legal lag is the inherent contradiction between "stability" and "dynamics" :

2.2.1 Legal attributes and tensions in the digital age

Disconnection between the legislative cycle and technological iteration: The Personal

Information Protection Law took five years from drafting to promulgation, while storage technology was upgraded from "traditional servers" to "cloud-native + edge storage" during the same period. Wang Luomei's (2025) risk assessment study pointed out that "the 'technology neutrality' principle of the legal provisions guarantees stability but cannot address new types of storage vulnerabilities, such as distributed ledger vulnerabilities at edge nodes." [2]

2.2.2 Structural deficiencies in regulatory capacity

Regulatory technology lags behind enterprise practice: Before 2019, China's cybersecurity regulators were only equipped with basic vulnerability scanning tools and were unable to detect hidden vulnerabilities in cloud storage (such as API logic flaws). According to Fu Sunyun (2025) 's research on data encryption, "at that time, regulatory authorities' inspection rate of the application of the national cipher algorithm SM4 was less than 30%, making it difficult to verify the effectiveness of enterprise storage security measures." [12]

2.2.3 Fuzzy breaks in the accountability mechanism

The dispute over the principle of imputation makes it difficult to hold accountable: The current law adopts the "principle of fault liability", and the determination of fault for storage vulnerabilities requires professional technical appraisal-in the 360 case, it took experts three months to confirm that "the configuration error is the fault of the enterprise", far beyond the statute of limitations. Xu Huaqing (2025) pointed out that "the law does not clearly define the 'static security' (not being leaked) and 'dynamic security' (legal transfer) interests of data storage, resulting in confusion of liability standards." [10]

2.3 Fault Superposition Effect: A Vicious Cycle of Exploitation of Technical Vulnerabilities and Failure of Legal Remedies

The "technology-legal gap" is not a static chasm but a dynamic and evolving vicious cycle system. The "low-threshold exploitation" of technical vulnerabilities and the "high-cost lag" of legal remedies add up to create a negative feedback that continuously exacerbates systemic risks to the security of personal information storage. The circular mechanism is manifested in four core links:

2.3.1 The "low-cost" exploitation of vulnerabilities and the "hollowing out" of legal deterrence reinforce each other

Technically, the popularity of automated attack tools such as Shodan scans and exploit frameworks and the maturity of the black industry chain have significantly lowered the technical and economic threshold for discovering and exploiting storage vulnerabilities. For instance, in 2019, storage exploit tools on the dark web cost as little as 500 yuan, allowing attackers to obtain high-value data with minimal investment. At the legal level, lagging legislation and ambiguous accountability have led to a serious lack of deterrence. Before the Data Security Law (2021) was introduced, the maximum fine for data breaches (500,000 yuan) was far lower than the security investment of enterprises and the potential gains of attackers, creating a distorted incentive of "cost of breaking the law < cost of abiding by the law". Yan Qi (2025) pointed out that "the hollowing out of legal deterrence directly stimulates the scaling and industrialization of vulnerability exploitation", accelerating the transformation of technical vulnerabilities from "potential risks" to "actual infringements".

2.3.2 The "negative incentive" of enterprise security investment resonates with the "probability" of legal accountability

Under the "technology-legal fault line", enterprises face an unbalanced calculation of security investment and legal risk. Due to the lack of technical standards, it is difficult for enterprises to define the boundaries of "necessary security measures," often cutting storage security budgets in pursuit of business efficiency. At the same time, the ambiguity of legal liability (such as the three months it took to complete the fault determination in the 360 incident) and the low probability of accountability have led companies to take chances that "even if something goes wrong, it will be difficult to hold them accountable." According to research by You Pengcheng (2025), "83% of small and medium-sized enterprises believe that the marginal benefit of safety investment is lower than the potential risk of fines", leading to a "race to bottom" of safety levels across the industry. This "negative incentive" allows security vulnerabilities to be systematically tolerated within enterprises, providing a breeding ground for external exploitation.

2.3.3 The "high speed" of technological iteration and the "periodicity" of legal updates create a speed difference

The iteration cycle of new storage architectures such as cloud-native and edge computing is measured in "months" or even "weeks", while the legal revision cycle can be several years. This speed gap leads to the lack of targeted regulatory provisions and effective detection tools for new vulnerabilities, such as container escape and API logic flaws, when they arise. Wang Luomei (2025) pointed out that "there is a regulatory vacuum of at least 2-3 years for the law to deal with new risks such as edge node distributed ledger vulnerabilities." Attackers take advantage of this vacuum period to launch "window period attacks" against new technology vulnerabilities, and legal remedies fall into a "no recourse" predicament due to the lack of basis, leaving victims with no way to protect their rights [2].

2.3.4 The "globalization" of cross-border data flows and the "territorialization" of legal jurisdiction have led to the failure of relief

In the context of global data flow, storage nodes may be distributed across different jurisdictions. When cross-border storage leaks occur (such as the Amazon S3 incident), victims face jurisdictional barriers and conflicts of application of law when seeking judicial relief in their home countries. At that time, our country lacked a GDPR-style "long-arm jurisdiction" mechanism and cross-border law enforcement collaboration channels, resulting in regulatory authorities being "out of reach" and the judicial system being "out of reach". A comparative study by Zhao Ruhan (2025) confirmed that "the success rate of relief for cross-border data breaches is less than 15%, far lower than 42% for domestic incidents." The failure of such relief further incentivizes companies to store sensitive data in loosely regulated jurisdictions, creating a distorted pattern of "data safe havens" and "risk transfer" [1].

3. Build a Dual-track Approach of "Legalization of Technical Standards + Strengthening of Accountability"

3.1 Bridging the Gap: The Core Logic of an Active Defense System

The core of active defense lies in achieving a deep integration of technical standards and legal liability. The law should translate mature practices in storage security into mandatory norms, establish the basic principle that "violating technical standards is illegal", and fundamentally address the current reality of the lack of compliance basis and the difficulty in holding accountable. Article 32 of the EU GDPR explicitly requires enterprises to adopt appropriate technical measures such as encryption, and provides clear guidance for compliance practices. This legislative experience is worth learning from in our country.

3.2 Path 1: Legalizing Technical Standards-Anchoring the Bottom Line of Storage Security with Rigid Legislation

The legalization of technical standards essentially elevates the best technical practices in the field of storage security to generally applicable legal norms. Through the three-tier framework of "defining technical requirements-establishing certification mechanisms-strengthening compliance linkages", the core problem of enterprises having no way to comply and regulatory enforcement having no basis can be effectively solved. In the legislative process, the principle of balancing risk orientation and feasibility should be adhered to, covering key risk points in the storage link comprehensively and taking into account the technical adaptation capabilities of enterprises of different sizes [18].

3.2.1 Define key technical requirements for storage: Build a security technology matrix for the entire life cycle

It is recommended that in the supporting administrative regulations of the Data Security Law (such as Data Security Technology-Personal Information Storage Security Specification), the storage security technical requirements be detailed into three modules: encryption protection, permission control, and vulnerability governance. Each module should have clear technical standards, implementation norms and acceptance indicators to form a mandatory requirement system that is implementable and verifiable to avoid the ambiguity of compliance caused by principle-based expressions [19].

3.2.2 Encryption standards: A full-link protection system centered on national cryptographic algorithms

Encryption is the first line of defense for the security of stored data. It is necessary to break the fragmented status of single-link encryption

and build a national encryption algorithm protection system covering the entire link of transmission, storage and use. The technical selection and specification design should take into account security, compatibility and domestic adaptation requirements. Legislation may enforce the use of SM4 block cipher (GB/T 32907-2016) as the benchmark algorithm for storing data encryption, which is comparable to AES in terms of anti-attack performance and runs more efficiently on domestic hardware such as Huawei Kunpeng chips and Phytium CPUs, and is more in line with the strategy of information technology autonomy and controllability. It is also necessary to specify the SM4 encryption mode (such as CBC mode for file encryption and CTR mode for stream data encryption) and the key management specification, requiring that the key length be no less than 128 bits and that the KMS key management system be rotated every 90 days [20].

For high-risk and sensitive data such as medical records, biometric data, and financial account information, full-link encryption measures need to be strengthened: use "TLS 1.3+SM4" double-layer encryption in the transmission link; "SM4 block encryption + transparent encryption (TEE)" is used for storage to ensure that data cannot be decrypted when the disk is stolen; "Dynamic desensitization +SM4 on-demand decryption" is used in the usage segment, such as restricting medical personnel to view only fragments of medical records within their permission and not landing the data. A tertiary hospital has reduced the risk of medical record data leakage from 12.7% to 0.3% through full-chain SM4 encryption transformation, confirming the effectiveness of the solution.

Legislation should also specify encryption compliance acceptance criteria: regulatory authorities can verify the effectiveness of encryption through black-box testing, requiring that the success rate of unauthorized cracking be less than 0.001%; check the integrity of rotation records and backup logs through key audits. Businesses that fail to meet the standards will be required to rectify within a specified period, during which sensitive data storage services will be suspended.

3.2.3 Permission control: Regulation of access boundaries centered on the principle of least privilege

The core of permission control is to prevent the risk of unauthorized access caused by excessive authorization. The principle of least privilege should be transformed into a technical specification covering the entire process of permission allocation, access verification, and operation auditing in light of the lessons learned from the Lenovo NAS incident. Permission allocation should establish a three-dimensional matching mechanism based on roles, data sensitivity, and business scenarios. First define basic permissions according to job roles, then refine the scope based on data sensitivity, and finally dynamically adjust the validity period of permissions in combination with business scenarios. For example, outpatient doctors can only access the general medical records of patients they have treated during the consultation period and have no right to view infectious disease medical records or historical data. At the same time, long-term super-administrator privileges are prohibited. The "temporary authorization + multi-person approval" model is adopted, such as system administrators modifying storage configurations requiring approval from more than two people in the information security department, and the authorization is valid for no more than 24 hours.

For critical access points such as API interfaces, administrator backends, and remote maintenance ports, two-factor and above authentication must be enforced, weak combinations such as "password + password hint" must be explicitly prohibited, and at least two of the knowledge factor, possession factor, and biological factor must be included. After the Lenovo NAS incident, the number of unauthorized access attempts dropped from 320 per day to zero by enabling triple authentication of password + dynamic token + IP binding. Legislation should also stipulate a mechanism for handling failed authentications, locking accounts after five consecutive failed authentications, and requiring manual review for unlocking to prevent brute-force cracking.

The access log is a key basis for tracing security incidents and should clearly record the content, retention period and tamper-proof measures: the recorded content should cover the access subject, time (accurate to milliseconds), behavior, object, terminal information and authentication result; The retention period should be no less than six months, with local and off-site backups for the first three months; Blockchain evidence storage or regular verification of hash values is used to

ensure the authenticity and completeness of logs, and the relevant provisions of Article 47 of the Personal Information Protection Law can be referred to for legal and technical connection.

3.2.4 Vulnerability detection: AI-driven dynamic scanning and emergency response mechanism

The dynamics of stored vulnerabilities make traditional manual detection difficult to deal with. Legislation requires enterprises to deploy AI vulnerability detection systems to build a closed-loop governance mechanism of real-time monitoring, automatic early warning, and rapid repair, focusing on three core indicators: detection coverage, response timeliness, and repair effectiveness. The system should include core modules such as asset mapping, vulnerability scanning, risk assessment, and automatic early warning. It is recommended to use advanced algorithms such as graph neural networks (GNN) and convolutional neural networks (CNN), which have a significantly higher recognition rate for component-associated vulnerabilities than traditional tools. In terms of detection frequency, for general storage systems, a full scan should be conducted at least once a week, while for sensitive data storage systems, a full scan plus real-time incremental scan should be conducted daily.

Different repair time limits should be set based on vulnerability severity levels: high-risk vulnerabilities (CVSS score ≥9.0) should be repaired within 24 hours, medium-risk vulnerabilities (CVSS score 6.0-8.9) within 72 hours, and low-risk vulnerabilities (CVSS score < 6.0) within 7 days. Upon discovery of the vulnerability, the system must immediately generate an emergency report containing the location of the vulnerability, hazard description, repair plan, and responsible person. The responsible person initiates the repair within one hour, and after completion, the AI system conducts a secondary scan verification and submits the "Vulnerability Repair Verification Report". For high-risk vulnerabilities that cannot be fixed within 24 hours, temporary control measures such as isolating nodes, suspending business, and enabling backups should be taken. A certain e-commerce platform used this mechanism to isolate high-risk vulnerability nodes within 15 minutes and complete the repair within 8 hours without causing data leakage.

To avoid formalized deployment by enterprises, a third-party assessment mechanism should be established: the effectiveness of the AI detection system should be evaluated annually by a nationally recognized cybersecurity testing agency, with core indicators including vulnerability identification accuracy ≥85%, false alarm rate ≤5%, and early warning timeliness ≤10 minutes. Enterprises that fail the assessment are required to rectify within a specified period and entrust a third party to provide vulnerability detection services during the rectification period.

3.2.5 Establish a mechanism linking technical certification to compliance: Achieve precise supervision and incentives for compliance through tiered certification

The implementation of technical standards should rely on the linkage mechanism of certification, regulation and incentives, referring to the classification logic of Cybersecurity Level Protection 2.0 (GB/T 22239-2019), to build a storage security certification system that matches data sensitivity. Through differentiated certification requirements, tiered regulatory measures, and positive compliance incentives, enterprises are guided to proactively implement technical standards, reducing the compliance burden brought about by one-size-fits-all regulation.

3.2.6 Construction logic and hierarchical division of the hierarchical certification system

Storage security certification should follow the principle that "the higher the data risk, the stricter the certification requirements", and be divided into three levels based on data sensitivity to achieve a precise match of levels, risks, and measures:

Level 1 certification is applicable to public data storage. The core requirements include basic SM4 encryption in the storage process, single-factor authentication in the administrator background, manual vulnerability scanning once a week, document review + remote detection, certification cycle of one year, simplified annual review process; Level 2 certification is for personal general information storage. It enhances full-link SM4 encryption, two-factor authentication for all access points, AI detection system with full scanning once a week, 6 months of blockchain evidence logs, uses document review + remote detection + on-site spot checks, has a certification period of 2 years, and submits semi-annual security assessment reports each year. Level 3 certification is applicable to the storage of personal sensitive information and core data. It requires full-link SM4+SM3 hash algorithm encryption, triple factor authentication

at key entry points, AI detection system with daily full + real-time incremental scanning, 1 year off-site double backup + third-party audit log and quarterly penetration testing. It uses full-process verification and has a certification period of three years. Each year, a third-party security assessment is required, and a storage security status report must be submitted every six months.

3.2.7 Linkage mechanism of certification and regulation: Differentiated regulation and penalties for breach of trust

Legislation should make it clear that "certification level determines regulatory intensity", encourage enterprises to upgrade their certification level through compliance exemptions, and restrain uncertified or non-certified enterprises through heavier penalties, forming a regulatory loop of positive guidance and reverse restraint. Enterprises that pass the level 3 certification can enjoy benefits such as reduced regulatory frequency, simplified approval process, priority policy support, such as reduced regulatory frequency from quarterly inspection to annual off-site verification, shortened storage system change approval time from 20 working days to 5 working days, priority qualification for government procurement and policy subsidies, etc. After a medical technology company passed the level 3 certification, its regulatory inspection frequency was reduced by 75% and it successfully won the bid for the provincial medical data platform project, demonstrating the incentive effect of certification.

For enterprises that fail to apply for certification as required, on-site inspections will be conducted once a month based on the highest risk level and they will be ordered to certify within a limited time. If the certification fails or expires without renewal, the sensitive data storage business shall be suspended and rectified within 30 days; if it still fails, a variable fine of 500,000 to 5 million yuan shall be imposed; In case of data breach due to failure to certify, civil liability shall be doubled on the basis of the fine. An e-commerce platform was fined 3 million yuan and paid 20 million yuan in compensation for leaking 500,000 pieces of user information without applying for secondary authentication. Legal deterrence can be strengthened by referring to Article 59 of the Cybersecurity Law.

3.2.8 Practical reference and legislative transformation of the authentication mechanism: Localized design based on the AWS case

After the Amazon S3 incident, AWS's storage security compliance certification provided a practical reference for China, but this certification was a commercial certification voluntarily participated by enterprises and needed to be transformed into a mandatory national certification system through legislation. The key points of the transformation include: First, legalization of the certification body, designating the National Cybersecurity Level Protection Work Coordination Group as the supervisory body, authorizing China Cybersecurity Review Technology and Certification Center and others as statutory certification bodies, stipulating that certification bodies must have more than 20 registered cybersecurity engineers and national-level testing laboratories, and bear joint and several liability for inaccurate certification results; Second, standardize the certification process. Transform "application-review-testing-certification-annual review" into a legal procedure. It is stipulated that the initial review of materials shall be completed within 10 working days after the enterprise's application, the testing shall be completed within 30 working days, the certification shall be issued within 15 working days, and the annual review shall be initiated 30 days in advance. At the same time, a review mechanism for objections and appeals within 15 working days shall be established. Third, mutual recognition and alignment of certification results: Establish mutual recognition mechanisms with international certifications such as CE of the European Union and FCC of the United States to avoid duplicate certification, and align the Level 3 storage security certification with the storage security requirements of Level 3 and above of the Information Security Protection 2.0 to reduce compliance costs for enterprises. After a multinational company passed China's Level 3 certification, its EU branch directly enjoyed mutual recognition treatment, reducing compliance costs by 40%.

3.3 Path 2; Bridging Step Legal Liability

3.3.1 Improve the criminal liability system

It is suggested that the crime of "refusing to fulfill the obligation of data storage security" be added to the Criminal Law, and the person in charge of enterprises who fail to implement mandatory technical standards and result in data

leakage be sentenced to fixed-term imprisonment or fined. The CEO of a medical company was sentenced to one year in prison for failing to enable storage encryption, which led to the leakage of millions of medical records, creating an effective deterrent.

3.3.2 Implement gradient administrative accountability

Set gradient fines based on the scale of the data breach and the degree of fault: A general breach (< 100,000 entries) will be fined 500,000 to 2,000,000 yuan; Major breaches (100,000 -1 million records) are fined 2 million -5 million yuan and subject to business restrictions; A particularly serious leak (more than 1 million pieces) will result in a fine of 5 million to 20 million yuan and the revocation of the business license. In 2024, an e-commerce platform was fined 3 million yuan for leaking 500,000 user data due to incorrect bucket configuration, which is more deterrent than previous fixed fines.

3.3.3 Introducing restorative civil liability

Require responsible enterprises to undertake technical repair obligations, such as providing two years of free credit monitoring services to affected users after the 360 incident, and publicly store security improvement roadmaps. Restorative liability can make up for the losses of the victims and push enterprises to improve their security level, which is more effective than simply imposing fines [16].

4. Contextualized Implementation Paths of Dynamic Compliance Frameworks

4.1 Implementation Strategies for Commercial Storage Scenarios

4.1.1 Tiered storage based on data heat

Referring to Zhou Jie's research results in the field of cloud computing security (2025), data can be classified into three levels based on access frequency: hot, warm, and cold. Hot data refers to data with access records within 30 days [17]. It requires high-performance storage devices combined with SM4 algorithms for real-time encryption, and an AI abnormal access monitoring system should be simultaneously enabled to ensure the security and controllability of the data interaction process. Warm data is data with access frequencies ranging from 30 to 90 days, and a hybrid storage architecture can be used to balance security and cost. Cold data is archived data that has not been accessed for more than 90 days and should be archived to offline storage media, along with multiple backup mechanisms and regular vulnerability scanning processes. After implementing this strategy, a leading domestic e-commerce company not only reduced its storage security operation costs by 25%, but also shortened the average vulnerability response time from 3 hours to 1 hour, achieving a dual improvement in security protection and operational efficiency.

4.1.2 Technical embedding of compliance requirements

The core idea is to promote the deep integration of compliance requirements with storage technology products, with cloud service providers pre-setting compliance baselines in the storage product system. Take Alibaba Cloud as an example. It has built-in control points related to Cybersecurity Level Protection 2.0 in its core storage products, covering more than 1,200 items, which can automatically identify sensitive information in stored data and trigger mandatory desensitization processes. The research data of Chen Jing (2025) shows that this model of technical embedding of compliance requirements can reduce the cost of enterprise compliance construction by 40%, effectively avoid problems such as "paper compliance" and "formal compliance", and ensure that compliance requirements are truly implemented.

4.2 Special Considerations for Government and Public Power Scenarios

4.2.1 Full application of the domestic technology stack

Government data storage is directly related to public interests and national security. Therefore, government storage systems must fully adopt domestic technology stacks, with core components including domestic chips such as Huawei Kunpeng, Kirin series operating systems, and domestic databases such as Kingbase, to prevent potential security vulnerabilities in the supply chain from the root. In 2024, a provincial government cloud platform suffered a data breach due to the use of foreign brand storage devices. Subsequently, the province fully promoted the substitution of domestic storage systems. After the substitution was completed, the rate of system security vulnerabilities decreased by 68% compared to before, fully demonstrating the security value of domestic technology stacks in government scenarios.

4.2.2 "Supervision +" collaborative governance mechanism

It is necessary to establish a collaborative process involving multiple departments, such as cyberspace administration, discipline inspection and supervision, and public security, with a focus on achieving two core functions: First, mutual transfer of clues, that is, clues of storage security vulnerabilities discovered by various departments in the course of performing their duties can be quickly transferred to the corresponding regulatory authorities for handling; Second, mutual recognition of evidence, unified standards for the collection and fixation of electronic evidence related to storage security to avoid obstacles in the connection of evidence in cross-departmental case handling. After the implementation of this collaborative mechanism in a prefecture-level city, the average time for handling cases of government data breaches has been shortened from three months to one month, significantly improving the efficiency of case handling and regulatory effectiveness.

4.3 Coordination Plan for Cross-Border Data Flow Scenarios

4.3.1 Dynamic management mechanism for negative list

Coordinate data security with the need for cross-border flows, establish and dynamically update a negative list of data outbound, and explicitly include core sensitive data such as medical and health records and biometric data in the prohibited outbound category. In open pilot areas such as Lingang, Shanghai, explore the implementation of the "filing system for data outside the list" reform, significantly simplifying the filing process for non-sensitive data outside the list, reducing the filing cycle from three months to 15 days. In 2024, a biopharmaceutical company successfully achieved the safe and orderly flow of cross-border research and development data with the help of the filing mechanism, and no data breach occurred throughout the year, providing a practical example for data security management in cross-border research cooperation.

4.3.2 Construction of a trusted technology assurance system

The core is to build a cross-border trusted data flow space, relying on technical means to resolve the contradiction between "data security" and "free flow". Specifically, blockchain technology can be used to achieve full traceability of cross-border data flows, ensuring that the data flow trajectory is traceable and verifiable; In combination with privacy computing technologies such as federated learning, build a security barrier of "data available but not visible" to achieve cross-border data value mining while safeguarding the rights and interests of data owners. Zhao Ruhan (2025) pointed out that the trusted technology system can effectively address security concerns in cross-border data flows. Currently, China and the EU have carried out pilot projects of mutual recognition of relevant technical standards in key areas such as intelligent connected vehicles, providing beneficial explorations for the standardization and security of cross-border data flows.

5. Conclusions

The "technology-legal gap" in the storage of personal information is essentially the core contradiction of security governance in the digital age, and its resolution requires breaking away from the traditional thinking of "technology for technology, law for law". The two-track approach of "legalization of technical standards + strengthening of responsibility" proposed in this paper achieves a governance transformation of "active defense" by converting technologies such as national encryption and AI detection into legal requirements and combining them with a stepwise responsibility mechanism; The scenario-based implementation approach provides precise solutions tailored to the differences in commercial, government, and cross-border scenarios. In the future, it is necessary to further promote the application of regulatory technologies (such as AI regulatory platforms), improve the criminal law regulation of data crimes (such as adding specific charges), and ultimately build a "technology-law-regulatory" coordinated storage security governance system to lay a solid security foundation for the healthy development of the digital economy.

References

[1] Zhao Ruhan, Chen Junxu. A Comparative Study of Cyberspace Governance in China, the United States and Europe: Experience, Challenges and Future Games [J/OL]. New media and society, 1-13 [2025-11-16]. https://link.cnki.net/urlid/CN.20251031.1731.002.

[2] Wang Luomei. Research on Cybersecurity

Risk Assessment Model in the Internet of Things Era [J]. Information recording materials, 2025, 26 (11) : 203-205.
[3] Tai Xiaoning. Application and Research of Computer Network Security and Vulnerability Scanning Technology [J]. Network Security Technology and Application,2025,(10):25-28.
[4] Chen Jing. Discussion on Computer Network Security Technology and Preventive Measures in the Era of Big Data [J]. And innovation of science and technology, 2025, (19) : 98-100 + 104.
[5] Tan Xin. Application Scenarios and Paths of Artificial Intelligence Technology in Computer Network Security [J]. Paper Equipment and Materials, 2020,54(09):100-102.
[6] Zhang Jing, Wu Xiaohui, Wu Mengdie. Computer network security protection technology based on intrusion detection [J]. Journal of electronic design engineering, 2025 (17) : 42-46.
[7] You Pengcheng. Research on the Application of Data Encryption in Computer Network Security Protection [J]. Software, 2020,46(07):184-186.
[8] Gao Yang. Computer Network Information Security Protection Based on Artificial Intelligence technology [J]. Encyclopedia Knowledge,2025,(21):11-13.
[9] Yan Qi. Research on Criminal Law Regulation of Data Crimes in the Digital Economy Era [D]. Shanxi University of Finance and Economics,2025.
[10] Xu Huaqing. Data the improvement of the crime of criminal law regulation research [D]. Yantai university, 2025.
[11] Chen Kunling, Li Chaoyu. Integrated Application of "Artificial Intelligence +" technology in Information Security [J]. Digital Technology and Applications, 2020,43(05):69-72.
[12] Fu Sunyun. Data encryption technology in Computer Network Security protection [J]. Information and Computer, 2020,37(08):93-95.
[13] Zhao Bo, Yang Le, Ding Yanqing, et al. Research and status analysis of Data Encryption Storage and Authentication algorithms [J]. Network Security Technology and Application,2025,(04):47-51.
[14] Chen Lin. Research on Legal Regulation of Personal Network Information Security Based on Face Recognition [J]. Ezhou university journal, 2025, 32 (02) : 12-15.
[15] Ren Yanjun, Ge Xiaoyong. Data crime criminal law regulation of the path optimization analysis [J]. Journal of Beijing institute of police, 2025, (3) : 29-37.
[16] Bai Peng, She Junjie, Li Ming, et al. Analysis of Computer Network Security Issues in the Information Age [J]. Digital Technology and Application, 25,43(01):55-57.
[17] Zhou Jie. Data Security and Privacy Protection Strategies for Electronic Components in Cloud Computing Environment [J]. Electronic and information technology, 2025, 9 (01) : 4-6 + 9.
[18] Ren Hong, Zhao Fan. A Review of security Vulnerability detection techniques for smart contracts [J]. Computer Applications,2024,44(S2):95-100.
[19] Wang Sai. Research on Maintenance and Management Measures of Computer Network Security in the Big Data Era [J]. Network Security and Informatization,2024,(10):158-159.
[20] Zhu Hao. Analysis of Information Security Issues and Prevention Strategies of Computer Network Technology in the Era of Big Data [J]. Information recording materials, 2024, 25 (09) : 43-45.

