Article

Research on Risk Review and Collaborative Governance of Personal Data Security in the Context of Big Data

Xiaona Liu[1,*]

[1] Hainan Vocational University of Science and Technology, Haikou, China
* Correspondence: Xiaona Liu, Hainan Vocational University of Science and Technology, Haikou, China

Abstract: The extensive application of big data technology has generated massive amounts of personal data across diverse sectors. While empowering the digital economy and enhancing social governance capabilities, this technological advancement simultaneously exposes personal data security to systemic risks throughout the entire data lifecycle, encompassing collection, storage, usage, analysis, sharing, and circulation stages. Drawing on contemporary regulatory frameworks and judicial practices, this paper systematically analyzes the risk manifestations and underlying root causes at each stage of the data lifecycle, identifying the current fragmentation and static nature of existing protective measures. The analysis reveals that conventional approaches to personal data protection remain predominantly reactive, lacking the dynamic coordination necessary to address evolving threats in the big data environment. Building on this foundation, the study proposes a multidimensional collaborative governance framework centered on the data lifecycle, integrating legal oversight, technical safeguards, corporate self-discipline, and user empowerment as interconnected pillars. A dynamic coordination mechanism spanning the entire data processing chain is designed to facilitate seamless cooperation among government agencies, technology enterprises, and individual users. This integrated approach aims to shift personal data protection from passive compliance toward proactive trust-building, thereby establishing a more resilient and adaptive security ecosystem. The proposed framework provides both theoretical foundations and practical references for safeguarding personal data in the big data era, contributing to the sustainable development of the digital economy.

Keywords: big data; personal data security; data lifecycle; collaborative governance; risk management

1. Introduction

Big data has emerged as a foundational strategic resource that underpins the advancement of the digital economy and supports the enhancement of social governance precision. The vast volume of personal data generated continuously through online interactions—including e-commerce transactions, social media engagement, mobile application usage, and smart device connectivity—constitutes an indispensable element for innovation, public service optimization, and evidence-based policy formulation. As the economic and societal value of such data intensifies, challenges related to over-collection beyond functional necessity, unauthorized disclosure due to inadequate technical safeguards or procedural lapses, inappropriate deployment of algorithmic systems in decision-making contexts, and illicit trading of personal information on underground platforms have grown in frequency and complexity. Personal data security risks now manifest across interconnected domains and institutional boundaries, posing significant threats to individual rights and interests while undermining trust in digital infrastructure and service ecosystems. Contemporary scholarly inquiry tends to concentrate on isolated protective mechanisms—such as consent management at data collection or encryption during storage—without adequately examining how risks propagate dynamically across acquisition, processing, sharing, retention, and deletion

Received: 02 July 2025
Revised: 15 August 2025
Accepted: 28 August 2025
Published: 31 August 2025

phases [1]. There remains a notable absence of an integrated governance architecture capable of aligning regulatory oversight, industry self-regulation, technological accountability, and public participation. This fragmentation leads to static, siloed interventions that lack adaptability and responsiveness to evolving threat landscapes. To bridge this gap, this paper adopts a comprehensive data lifecycle perspective, conducts in-depth analysis of risk patterns at each operational stage using empirically grounded case examples, and proposes a multidimensional collaborative governance framework featuring adaptive coordination protocols, role-based responsibility allocation, and real-time feedback loops. The framework is designed to strengthen systemic resilience while enabling responsible data utilization and robust privacy preservation.

2. Risk Assessment of Personal Data Security in the Context of Big Data

In the era of big data, personal data security risks have significantly intensified and diversified compared to traditional information environments [2]. Data collection practices are no longer confined to specific purposes or predefined scopes; instead, they operate pervasively across digital platforms, IoT devices, and service ecosystems. Technological capabilities increasingly enable continuous, granular, and often invisible acquisition and long-term retention of personal information. The intrinsic value of personal data is frequently realized not in isolation but through large-scale aggregation, cross-domain linkage, algorithmic analysis, and iterative reprocessing—rendering repeated reuse an inherent feature of modern data economies. This paradigm introduces layered vulnerabilities: at the collection stage, consent mechanisms may lack transparency or meaningful control; during storage, inadequate encryption or access governance increases exposure; in processing, opaque analytics may produce discriminatory outcomes; and upon sharing or transfer, fragmented regulatory oversight compounds accountability gaps. These interdependent threats reinforce one another, forming self-perpetuating risk cycles that challenge conventional security frameworks and necessitate holistic, lifecycle-aware governance strategies grounded in technical robustness, legal compliance, and ethical responsibility.

2.1. Power Imbalance Becomes Prominent, with Informed Consent Reduced to a Formality

Data collection constitutes a foundational source of personal data security challenges, with the underlying structural issue being an asymmetrical relationship between data collectors and individuals. This imbalance significantly undermines the practical implementation of the informed consent principle. Users routinely encounter lengthy, complex, and technically dense privacy policies that are difficult to comprehend, resulting in superficial rather than meaningful consent. The prevailing 'accept-or-forego-service' framework effectively eliminates genuine user autonomy, as refusal typically leads to denial of essential digital or physical services [3]. Driven by competitive market dynamics, certain entities engage in excessive data acquisition—collecting information beyond functional necessity—and retain such data for extended durations without transparent justification, thereby increasing exposure risks and complicating accountability mechanisms. Such practices reflect broader systemic tensions between service convenience, commercial imperatives, and individual data rights.

Empirical observations reveal recurring concerns regarding offline biometric data collection, particularly through facial recognition systems deployed in retail environments and public tourism venues. Regulatory oversight bodies have emphasized the importance of transparency, purpose limitation, and user choice in such deployments. Instances where devices operate without clear signage, fail to specify data usage purposes or retention timelines, and offer no non-biometric alternatives have drawn formal attention from competent authorities. Similarly, digital service interfaces—including QR code–based food ordering platforms and mandatory subscription requirements for official accounts—frequently request personal details unrelated to transaction fulfillment [4, 5]. Market supervision departments have clarified that such demands contravene statutory protections for consumer autonomy and data minimization principles.

Furthermore, the instrumentalization of personal information for commercial advantage—without explicit, granular, and revocable authorization—introduces cumulative vulnerabilities across the data lifecycle, necessitating strengthened governance frameworks, technical safeguards, and continuous compliance monitoring to uphold lawful, fair, and transparent processing standards.

2.2. Double Attack of Technical Vulnerabilities and Internal Threats

The core risk in data storage arises from the concurrent presence of suboptimal technical configurations and insufficient internal governance mechanisms, which collectively undermine the intended protective function of data infrastructure and increase exposure to unauthorized access incidents. Databases aggregating large-scale user information face heightened operational complexity, requiring robust architectural design, continuous monitoring, and adaptive security controls [6]. Outdated encryption protocols, inconsistent access control policies, and misaligned system parameter settings may contribute to unintended data exposure scenarios. Personnel with authorized system privileges represent a critical dimension of risk management—organizational oversight must ensure strict role-based authorization, comprehensive audit logging, and periodic competency verification. Traditional centralized storage models inherently concentrate responsibility and failure impact; when compounded by fragmented accountability structures and inconsistent implementation of security standards across departments, systemic resilience diminishes. In judicial proceedings, a mobile application enterprise was held legally accountable for improper handling of user information, stemming from absence of standardized identity authentication procedures and inadequate safeguards during data retention phases. Regulatory disclosures by cyberspace administration authorities have also documented multiple cases involving internet enterprises where delayed remediation of known system configuration issues—due to limited technical capacity and insufficient security awareness—led to preventable unauthorized access events. These interrelated technical and procedural shortcomings reflect broader challenges in aligning infrastructure capabilities with evolving regulatory expectations and user protection requirements, ultimately affecting the integrity and confidentiality of personal information.

2.3. Algorithm Abuse as a Hidden Danger, De-Anonymization Brings New Risks

The core challenge in data utilization and analysis lies in privacy risks arising from the unregulated application of algorithmic systems and rapid progress in de-identification reversal techniques. Big data analytics enables the inference of sensitive attributes—including consumer behavioral tendencies, health-related indicators, and lifestyle patterns—through secondary analysis of seemingly non-sensitive datasets. Even datasets subjected to standard anonymization procedures may be vulnerable to re-identification when subjected to multi-source linkage, statistical inference, or auxiliary information integration. Moreover, the inherent opacity of many machine learning models—the so-called 'black box effect'—limits transparency in automated decision-making processes, potentially resulting in inconsistent, unjustified, or inequitable outcomes for individuals. Such limitations underscore the need for robust technical safeguards, rigorous governance frameworks, and continuous auditing mechanisms to ensure fairness, accountability, and interpretability across data-driven applications [7].

In practical deployment scenarios, certain digital educational platforms require users to provide personal information that bears no functional relationship to the primary educational service, effectively conditioning platform access on excessive data collection [8]. Judicial rulings have clarified that such requirements exceed the scope necessary for contract formation and performance, thereby violating statutory protections governing personal information handling. This jurisprudential precedent plays a pivotal role in shaping regulatory expectations and industry compliance standards. Concurrently, advances in computational analytics have significantly lowered the technical barriers to de-identification reversal: research efforts have successfully reconstructed granular user profiles by integrating geolocation traces, transaction records, and behavioral metadata—

even when original identifiers were formally removed. The cumulative effect of aggregating disparate, low-sensitivity data fragments amplifies systemic privacy exposure, necessitating enhanced legal, technical, and organizational controls aligned with evolving national data security and personal information protection requirements.

2.4. Uncontrolled Data Circulation Leads to Prominent Issues in Secondary Utilization

A key challenge in data sharing and circulation stems from the difficulty of maintaining consistent governance once data transitions across organizational boundaries. As data moves between platforms, institutions, or service providers, its original collection context—including purpose specification, consent scope, and usage limitations—often becomes diluted or obscured [9]. This operational complexity can result in deviations from intended use, including unregulated redistribution, unauthorized reuse for purposes beyond those originally authorized by data subjects, or the emergence of informal data exchange channels that operate outside formal compliance frameworks. Current oversight mechanisms face practical constraints in tracking data lineage and enforcing usage boundaries across heterogeneous technical environments and contractual arrangements. Consequently, personal data may be subject to aggregation practices that lack transparency, raising concerns about potential misalignment with statutory requirements for lawful, fair, and transparent processing. Such scenarios underscore the importance of strengthening technical traceability, enhancing contractual accountability, and deploying interoperable governance tools—such as purpose-limited data access controls and audit-ready metadata tagging—to support responsible secondary utilization while preserving individual rights and institutional trust.

Regulatory authorities have intensified efforts to address unlawful data acquisition activities, particularly those involving automated extraction techniques applied to publicly accessible digital interfaces. Instances have been documented where user behavioral patterns, transaction records, and profile attributes were systematically collected from e-commerce and social media platforms without proper authorization, subsequently repackaged or resold in fragmented or enriched forms. These practices pose significant challenges to privacy protection frameworks and introduce friction into fair competition dynamics within digital markets. Even within formally sanctioned data-sharing arrangements, users frequently encounter diminished visibility into downstream data handling due to layered intermediation and opaque contractual terms. This limits their ability to exercise statutory rights—including requests for data correction, deletion, or restriction of processing—especially when data undergoes multiple transfers across jurisdictional or functional boundaries. A representative example involved an online retail platform transferring customer contact and purchase history information to an external analytics vendor under a commercial agreement; the vendor subsequently deployed this information in targeted advertising initiatives without explicit re-consent, prompting regulatory review and consumer feedback. Such cases highlight systemic gaps in end-to-end data stewardship and reinforce the need for enforceable data use agreements, standardized data provenance documentation, and proactive user empowerment mechanisms.

3. Construction of Personal Data Security Governance Framework with Multi-Dimensional Collaboration

In the big data era, personal data security faces increasingly complex and systemic challenges that transcend the capacity of conventional protection strategies relying solely on isolated, post-incident interventions. A robust and adaptive governance approach must therefore be grounded in the full data lifecycle—from collection and storage to processing, sharing, and eventual deletion—while actively integrating diverse actors including regulatory authorities, technology developers, data controllers, industry associations, and individual data subjects. The foundational principle guiding this framework is collaborative synergy: it seeks to harmonize the dual imperatives of enabling responsible data utilization for socioeconomic advancement and upholding

fundamental privacy rights through proportionate, transparent, and accountable mechanisms. This requires not only complementary alignment among policy instruments, technical standards, organizational practices, and individual capabilities, but also dynamic feedback loops that allow continuous refinement of governance responses in light of evolving technological developments and societal expectations. The subsequent analysis systematically examines four interdependent dimensions—legal frameworks, technical safeguards, corporate accountability mechanisms, and user-centric empowerment strategies—while articulating how their coordinated operation sustains resilience across all stages of data handling (As shown in Table 1).

Table 1. Multidimensional Collaborative Governance Framework for Personal Data Security

Governance dimension	Core positioning	Core initiatives throughout the life cycle	key role
legal regulation	system safeguard	Define boundaries, clarify requirements, establish algorithmic oversight, create shared classification, and regulate retention and deletion	Draw the red line of rule of law and define the rights and responsibilities
technical protection	Technical Support	Traceability, Anonymity, Encrypted Traceability, Privacy Computing, Blockchain Traceability, Professional Destruction	Technology ensures full-process traceability
self-regulation	Core subject	Minimum data collection, approval and transmission, algorithm audit, standardized sharing, and periodic cleanup	Implementing primary responsibility and promoting proactive compliance
Empowering Users	Participate in oversight	Violation collection, informed consent, objection algorithm, authorization traceability, request deletion	Full-process supervision, forcing compliance

3.1. From Static Declaration to Dynamic Supervision: Strengthening Power Constraints

Legal frameworks constitute a foundational element in the governance of personal data security, necessitating an evolution from static articulation of entitlements toward continuous, process-oriented oversight and balanced institutional accountability across all stages of data handling. A robust regulatory architecture must span the full data lifecycle, structured around four interlocking pillars: precise definition of entitlements, real-time behavioral monitoring, institutional coordination mechanisms, and internationally aligned governance protocols. First, the entitlement framework for personal data should be systematically refined—building upon established statutory provisions—to explicitly recognize rights related to algorithmic transparency and user autonomy in automated decision-making contexts. Scenario-specific thresholds for permissible data collection should be calibrated through evidence-based analysis, drawing on authoritative judicial interpretations concerning proportionality and necessity. Second, regulatory emphasis must transition from procedural compliance with consent formalities to substantive evaluation of system design and operational outcomes. This entails institutionalizing mandatory algorithmic documentation, periodic technical assessments, and independent auditing procedures to ensure fairness, reliability, and accountability in algorithmic systems. Third, a dedicated oversight entity should be established under the national cyberspace administration, empowered with cross-sectoral coordination authority, investigative capacity, and enforcement tools—including corrective measures and administrative sanctions. Complementary legal pathways, such as public interest litigation, should be institutionalized with clearly defined standing criteria for authorized entities to enhance accessibility and reduce procedural barriers for individuals seeking redress. Finally, international data transfers should be governed by a

risk-proportionate classification scheme—categorizing data into general, sensitive, and critical tiers—each subject to distinct authorization, assessment, and monitoring requirements. Critical data is generally restricted from external transfer; sensitive data undergoes rigorous security verification; and general data operates under streamlined notification-based administration.

3.2. Implement Privacy-Conscious Design Principles and Fortify Security Barriers through Technology

Technical safeguards constitute a foundational element of personal data security governance, enabling a strategic shift from post-incident response toward proactive, privacy-by-design integration across the full system development and operational lifecycle. These safeguards must be embedded as mandatory default requirements and intrinsic functional components within product and system architectures—not as optional add-ons. Comprehensive risk mitigation should span all critical data handling stages: collection, storage, analysis, and sharing—thereby realizing the principle of 'governance through technological architecture'. During data collection, scenario-specific, fine-grained authorization frameworks should be deployed, supported by robust data lineage tracking mechanisms that log origin, purpose, scope, and consent status in real time; concurrently, sensitive data elements must undergo immediate pseudonymization or structural anonymization at ingestion to minimize exposure risks at the earliest possible point. In storage, adoption of domestically developed cryptographic standards—including SM4 for symmetric encryption and SM9 for identity-based encryption—is strongly encouraged; additionally, distributed ledger technologies may be explored to enhance resilience against centralized failure modes and unauthorized internal access, while preserving verifiable audit trails across all storage operations. During analytical processing, privacy-enhancing computation methods—including homomorphic encryption, differential privacy, and secure multi-party computation—should be systematically applied to enable high-fidelity statistical insights without exposing raw individual records, thus reconciling utility with confidentiality. Such approaches have demonstrated practical efficacy in regulated domains such as financial services and public administration. For data sharing, persistent digital watermarking combined with immutable provenance logging ensures each data instance carries a unique, tamper-evident identifier, enabling end-to-end circulation monitoring, accountability attribution, and automated compliance verification throughout its entire lifecycle.

3.3. From Passive Compliance to Proactive Responsibility: Building User Trust

As the core entities in data processing, enterprises play a pivotal role in safeguarding personal data security. Their self-discipline must evolve from passive compliance to proactive responsibility, building user trust by elevating data protection to a strategic priority and establishing comprehensive internal management systems covering the entire data lifecycle—from collection and storage to use, sharing, and secure disposal. Companies should develop internal security frameworks aligned with data scale, processing scope, and associated risks, implementing rigorous data classification standards, tiered access controls based on functional necessity, and strict minimum privilege access policies. Clear data protection responsibilities must be assigned to all positions across departments, with designated data security officers conducting regular risk assessments, timely remediation of identified issues, and systematic employee training programs grounded in national laws and regulatory requirements. Industry practices—including formalized data governance roles and privacy-preserving technical architectures—offer valuable references for domestic enterprises. Beyond formal compliance, organizations should optimize privacy policies through intuitive visual designs, plain-language explanations, and interactive interfaces that enhance user comprehension. The 'one-thing-one-authorization' model should be fully implemented, enabling users to independently manage permissions for non-core service data with granular control and real-time revocation capability. Furthermore, companies must proactively integrate privacy-by-design principles into product development lifecycles,

apply privacy-enhancing technologies such as anonymization, differential privacy, and secure multi-party computation, and embed data protection considerations at every stage—from requirement analysis and architecture design to testing and deployment. By transforming data protection into a core competitive advantage, enterprises can achieve sustainable development where robust data security practices reinforce business innovation, operational resilience, and long-term user loyalty.

3.4. From Passive Acceptance to Active Participation, Strengthening Subject Consciousness

As the primary data owners, users constitute direct stakeholders in data security governance. Empowering them necessitates a systematic shift from passive exposure to risks toward proactive engagement and oversight, achieved through differentiated, context-sensitive strategies. This transformation entails not only raising awareness of privacy-related considerations but also cultivating practical competencies across diverse demographic groups—such as older adults, adolescents, and working-age populations—while simultaneously optimizing accessible, responsive mechanisms for addressing concerns. Coordinated initiatives involving governmental agencies, cyberspace regulatory entities, and professional industry associations should deliver stratified data security literacy programs. Educational content and delivery modalities must be rigorously tailored: community-based seminars and face-to-face assistance for elderly users; curriculum-integrated instruction within formal education systems for students; and concise, mobile-optimized formats—including short-form video content and official public accounts on widely used platforms—for broader public outreach. Enterprises are expected to embed user-centric design principles into digital interfaces, enabling straightforward access to personal data, timely correction of inaccuracies, and seamless withdrawal of consent. Regulatory frameworks should support standardized, interoperable complaint handling systems featuring intuitive submission workflows and transparent progress tracking. Furthermore, transparency requirements for privacy notices mandate that businesses present essential data processing information in plain language, using visually salient, non-intrusive interface elements—thereby ensuring meaningful, functional consent rather than procedural compliance.

3.5. Dynamic Collaborative Mechanism Across the Entire Lifecycle

The four governance dimensions—legal frameworks, technical safeguards, corporate accountability mechanisms, and user participation channels—are inherently interdependent and must operate in coordinated alignment across the full data lifecycle. This lifecycle encompasses all stages: initial collection, secure transmission, responsible usage, controlled sharing, and final erasure. Each dimension contributes distinct yet complementary functions, collectively enabling a robust, adaptive, and responsive governance architecture. Rather than operating in silos, these dimensions reinforce one another to realize a comprehensive closed-loop system grounded in three core operational principles: anticipatory risk mitigation, continuous process monitoring, and timely corrective intervention. Such integration ensures that governance is not static or reactive but evolves dynamically with technological developments, organizational practices, and evolving stakeholder expectations. The resulting framework supports consistent policy implementation while allowing for contextual adaptation across sectors such as healthcare, finance, education, and public services.

1) Data Collection Phase: Emphasis is placed on foundational risk prevention through structured authorization protocols and systematic oversight. Statutory provisions delineate permissible scope, purpose limitation, and data minimization requirements, establishing clear operational boundaries. Regulatory authorities conduct periodic compliance assessments using standardized evaluation criteria and digital audit tools. Enterprises implement granular consent management systems aligned with the principle of data minimization, ensuring only essential information is collected for specified purposes. Technical infrastructure supports immutable logging of collection events—including time stamps, source identifiers, and processing logic—facilitating accountability and forensic traceability. Users receive transparent, accessible disclosures

regarding data collection purposes, retention duration, and downstream implications, empowering informed decision-making. This integrated approach synthesizes statutory parameters, regulatory verification, enterprise-level procedural rigor, technical auditability, and user-centered transparency into a cohesive preventive architecture that substantially reduces upstream vulnerabilities.

2) Data Transmission Phase: Focus shifts toward maintaining integrity and confidentiality throughout transfer operations. Legislative instruments specify security obligations for cross-system and cross-organizational data flows, including requirements for authentication, integrity verification, and channel protection. Domestic cryptographic standards and watermarking techniques are deployed to guarantee end-to-end confidentiality, detect unauthorized modifications, and support forensic attribution. Organizations enforce multi-tiered approval workflows for data transfers, incorporating risk scoring, recipient vetting, and contractual safeguards. Regulatory bodies deploy sector-specific monitoring platforms—particularly in critical infrastructure domains—to verify adherence to transmission protocols and identify anomalous patterns. Users receive timely notifications about transfer destinations, purposes, and legal bases, with mechanisms available to withdraw consent where transfers lack legitimate grounds. This layered strategy combines cryptographic assurance, statutory mandates, organizational gatekeeping, supervisory surveillance, and user notification rights to uphold transmission integrity and accountability.

3) Data Usage Phase: Governance intensifies through dual-layered oversight targeting both algorithmic logic and operational behavior. Legal instruments mandate documentation, registration, and periodic evaluation of automated decision-making systems, particularly those affecting individual outcomes. Judicial interpretation contributes to normative clarity by addressing emerging challenges in fairness, transparency, and contestability. Privacy-enhancing computation methods—including secure multi-party computation and differential privacy—enable analytical utility while preserving data confidentiality and minimizing exposure risks. Enterprises institutionalize internal review cycles for algorithm deployment, integrating bias detection, impact assessment, and documentation standards. Users possess accessible redress pathways to request explanations, challenge adverse decisions, and initiate human review where appropriate. This cooperative model integrates statutory algorithm governance, privacy-preserving engineering, enterprise diligence, judicial guidance, and user recourse mechanisms to ensure equitable and accountable data utilization.

4) Data Sharing Phase: Governance prioritizes lawful, auditable, and purpose-bound exchange. Legal classification schemes categorize data assets according to sensitivity, value, and societal impact, prescribing differentiated handling rules for each tier. Distributed ledger technologies and fine-grained metadata tagging enable immutable recording of sharing events—including participants, timing, scope, and contractual terms—supporting real-time visibility and retrospective analysis. Industry associations develop consensus-based guidelines for due diligence on sharing partners, including security posture verification and compliance history checks. Regulatory agencies operate centralized oversight dashboards offering cross-sectoral visibility into sharing activities, facilitating coordinated enforcement and trend analysis. Users retain explicit control over sharing permissions, with dynamic consent interfaces supporting granular, revocable, and time-limited authorizations. This multifaceted mechanism—integrating verifiable traceability, legally calibrated classification, industry-led due diligence, regulatory coordination, and user-directed authorization—ensures orderly, transparent, and accountable data circulation.

5) Data Erasure Phase: Governance culminates in verifiable, irreversible termination of data processing obligations. Statutory provisions define retention periods based on functional necessity, legal requirements, and sector-specific norms, mandating deletion upon expiration or withdrawal of consent. Enterprises embed automated cleanup routines within data management systems, incorporating validation checks to confirm complete removal from primary storage, backups, caches, and logs. Certified data sanitization

techniques—including cryptographic erasure and physical destruction protocols—are applied to prevent residual recovery. Regulatory inspections include targeted audits of deletion logs, retention schedules, and verification reports to assess compliance fidelity. Users may submit deletion requests via standardized interfaces and receive status updates confirming execution, including timestamps and methodological details. This holistic framework—anchored in statutory timelines, technical irreversibility, enterprise procedural discipline, regulatory verification, and user-initiated control—affirms the principle of data stewardship as a time-bound, accountable, and user-respectful responsibility.

4. Conclusion

In the era of big data, personal data security presents multidimensional challenges that span technological infrastructure, regulatory design, organizational practice, and individual agency. Risks are not isolated to discrete phases but permeate the entire data lifecycle—from collection and storage through processing, sharing, and eventual deletion—while simultaneously propagating across legal, technical, operational, and behavioral domains. Consequently, siloed interventions prove inherently inadequate. This paper systematically identifies and characterizes core vulnerabilities at each stage of the data lifecycle through rigorous practical analysis grounded in real-world deployment contexts. Building on this analysis, it proposes a collaborative governance framework explicitly structured around the temporal and functional logic of the data lifecycle. The framework integrates four interdependent dimensions: legal accountability mechanisms, robust technical safeguards, resilient organizational policies and accountability structures, and empowered user participation supported by transparency and meaningful control. Crucially, it incorporates dynamic coordination mechanisms—including feedback loops, adaptive policy triggers, and cross-domain alignment protocols—to bridge persistent fragmentation in current research and practice. This represents a paradigmatic shift from reactive, compliance-driven approaches toward proactive, trust-oriented governance. As emerging technologies evolve, new risk vectors—including covert data acquisition methods and vulnerabilities in cryptographic implementations—will necessitate governance models that embed anticipatory capacity and structural flexibility. Ultimately, effective governance hinges on sustaining a principled equilibrium between enabling responsible data utility and ensuring enduring privacy protection. Only through sustained multidimensional coordination, continuous learning, and context-sensitive adaptation can a comprehensive, future-resilient data security ecosystem be realized.

References

1. X. Chen, Y. Gao, H. Tang, and X. Du, "Research progress on big data security technology," *Scientia Sinica Informationis*, vol. 50, no. 1, pp. 25–66, 2020.
2. A. Mehmood, I. Natgunanathan, Y. Xiang, G. Hua, and S. Guo, "Protection of big data privacy," *IEEE Access*, vol. 4, pp. 1821–1834, 2016.
3. I. Rubinstein, "Big data: the end of privacy or a new beginning?," *International Data Privacy Law*, NYU School of Law Public Law Research Paper No. 12-56, 2012.
4. M. E. Kaminski and G. Malgieri, "Impacted stakeholder participation in AI and data governance," *Yale Journal of Law and Technology*, forthcoming 2024–2025, U. of Colorado Law Legal Studies Research Paper No. 24-23, 2024.
5. W. Fang, X. Z. Wen, Y. Zheng, and M. Zhou, "A survey of big data security and privacy preserving," *IETE Technical Review*, vol. 34, no. 5, pp. 544–560, 2017.
6. D. Zhang, "Big data security and privacy protection," in *Proc. 8th Int. Conf. Manage. Comput. Sci. (ICMCS 2018)*, Atlantis Press, Oct. 2018, pp. 275–278.
7. L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: privacy and data mining," *IEEE Access*, vol. 2, pp. 1149–1176, 2014.
8. G. Lafuente, "The big data security challenge," *Network Security*, vol. 2015, no. 1, pp. 12–14, 2015.
9. J. Moura and C. Serrão, "Security and privacy issues of big data," in *Handbook of Research on Trends and Future Directions in Big Data and Web Intelligence*, IGI Global Scientific Publishing, 2015, pp. 20–52.