Trends in Social Sciences and Humanities Research
Print ISSN: 2959-992X
Online ISSN: 2959-9938
DOI: https://doi.org/10.61784/tsshr3252

THE ALLOCATION OF POWERS AND RESPONSIBILITIES IN GOVERNMENT DATA SHARING AMID DIGITAL GOVERNMENT DEVELOPMENT

Nan Li
Institute of Law, Shandong Academy of Social Sciences, Jinan 250000, Shandong, China.

Abstract: Government data sharing is not merely a matter of data transmission or technical connectivity; it entails a reconfiguration of the boundaries of administrative authority, interdepartmental coordination, and the structure of data-related risks in the development of digital government. Traditional bureaucratic organization rests on departmental division of functions, whereas digital government requires data to move across organizational boundaries, generating a structural tension between department-based allocation of authority and the demands of holistic governance. Existing scholarship discusses government data sharing from the perspectives of digital government, data governance, interagency collaboration, sharing security, and administrative rule of law, yet still lacks a unified account of the correspondence among data-management authority, sharing duties, use permissions, and legal responsibility. The allocation of powers and responsibilities in government data sharing should neither continue the logic of departmental possession of data nor attribute responsibility simply according to who supplies or ultimately uses the data. Instead, statutory tasks should define the boundaries of authority, actual control capacity should determine conduct-based duties, and causation and degree of fault should guide the internal allocation of responsibility. On this basis, it is necessary to distinguish the coordinating responsibility of the competent sharing authority, the data-quality responsibility of source departments, the sharing-service responsibility of providing departments, the administrative-use responsibility of requesting departments, and the technical safeguarding responsibility of platform operators, while establishing a structure in which external responsibility is relatively unified and internal responsibility is allocated in layers. Future reform should reconstruct data-management authority, refine layered standards of responsibility, improve whole-process matrices of powers and responsibilities and mechanisms of traceability, and develop an accountability regime that addresses both failures to share and unlawful use, thereby reconciling efficiency, security, and responsibility in government data sharing.
Keywords: Digital government; Government data sharing; Allocation of powers and responsibilities; Institutional collective action; Administrative responsibility

1 INTRODUCTION

Digital government development is not simply the digitization of conventional administrative activities; rather, it represents a transformation in governmental operation produced by the deep integration of digital technologies, data resources, and administrative organization. While digitization enhances information-processing capacity, it also reshapes interdepartmental relations and resource allocation. Traditional bureaucratic systems allocate administrative authority according to functional specialization, with each department separately collecting, managing, and using information related to its statutory remit. Digital government, by contrast, requires data to flow across levels of government, regions, systems, and departments in response to public-governance tasks and the needs of businesses and citizens [1]. Zhang Chengfu and Xie Kankan argue that digital government development entails not a localized technological improvement but a systemic transformation of organizational form, operating mechanisms, and modes of governance; Huang Huang similarly identifies data-driven operation, platform integration, and organizational collaboration as its defining features [2-3]. Research on digital-era governance and whole-of-government reform likewise shows that information technology can weaken the constraints that organizational boundaries impose on business processes, but it cannot automatically remove departmental divisions, power structures, or institutional inertia. Digital reform must therefore proceed together with the adjustment of organizational rules and systems of responsibility [4-6]. The central difficulty of government data sharing, accordingly, lies not merely in building a unified platform or connecting data interfaces, but in reallocating existing powers, duties, and responsibilities once data cross departmental boundaries.

Existing research on government data sharing has broadly followed three analytical paths. The first approaches the issue from digital government and governmental data governance, focusing on departmental barriers, data standards, organizational coordination, and life-cycle management. Bao Jing and Zhang Yongjin regard data governance within government departments as both a technical and an organizational problem; Huang Huang uses the perspective of data flows to reveal the relationships among governance actors, rules, and processes. Xu Xiaolin et al., Li Chongzhao and Huang Huang, and Yuan Gang et al. further examine the determinants, practical obstacles, and organizational conditions of local-government data sharing [7-11]. The second path focuses on collective action and coordination

mechanisms in interagency sharing. Dawes observed early on that government information sharing produces both public benefits and managerial risks, and that agency participation depends on an overall assessment of benefits, costs, and risks. Yang and Maxwell, Gil-Garcia and colleagues, and related studies identify organizational trust, leadership support, institutional environment, and technical capacity as major determinants of interagency information sharing [12-14]. Feiock's theory of institutional collective action further explains that when governing authority is dispersed across organizations and the costs and benefits of one actor's conduct spill over to others, interorganizational cooperation is burdened by coordination costs and risks of opportunism [15]. The third path examines the legal basis, limits, data security, and protection of individual interests under administrative law and data law. The focus of this scholarship has gradually shifted from whether government data should be shared to the legal governance of digital administrative power, the risks of government-data aggregation, and the administrative-law foundations of public-data sharing [16-22]. Although these studies provide important foundations, two gaps remain. First, many accounts treat the allocation of powers and responsibilities as a static list of departmental functions and do not adequately reveal deeper structures, including the socialization of sharing benefits, the departmentalization of risk, and the separation between statutory authority and factual control. Second, insufficient distinction is drawn between external responsibility for administrative consequences caused by erroneous data and the internal allocation of responsibility within government, leading to a formalistic choice between “whoever manages is responsible” and “whoever uses is responsible.” Taking the current institutional framework established by the Regulations on Government Data Sharing as its normative background, this article integrates whole-of-government theory, institutional collective action, and digital administrative rule-of-law theory to construct a task-control-causation framework for explaining the relationships of power, duty, and responsibility among the principal actors in government data sharing and for proposing corresponding institutional reforms [23].

2 THEORETICAL FOUNDATIONS FOR ALLOCATING POWERS AND RESPONSIBILITIES IN GOVERNMENT DATA SHARING

2.1 Structural Tension between Departmental Specialization and Holistic Governance

Modern administrative organization is based on specialized division of labor. Different government departments perform public-management and service functions in accordance with statutory mandates, and departmental boundaries are both organizational conditions for professional administration and rule-of-law requirements for constraining power and identifying responsible actors. The integrated coordination pursued by digital government does not imply abolishing departmental divisions. Instead, it seeks to overcome fragmented governance through data flows and business-process collaboration while retaining statutory boundaries of competence. Whole-of-government theory arose in response to organizational segmentation, fragmented responsibilities, and service disconnection associated with New Public Management. Its core is not the creation of an undifferentiated omnibus department, but the use of vertical coordination, horizontal collaboration, and process integration to enable different organizations to cooperate consistently around common governance objectives [5-6]. In government data sharing, the tension between departmental specialization and holistic governance appears in several ways. Data are generally generated by particular departments in the course of their duties, yet their governance value may emerge only when they are used by other departments or combined with other data. Data-managing departments understand data meanings and update rules, but cannot necessarily assess every use scenario; requesting departments possess substantive administrative authority, but do not control data formation. Powers and responsibilities therefore cannot be allocated solely according to where data are held. Data management, sharing decisions, and administrative use must be reconnected without altering the statutory allocation of administrative functions. The institutional task of digital government is not to replace specialization with technological integration, but to lower interdepartmental coordination costs through clear allocations of power and responsibility, thereby aligning data flows with administrative authority [2-4,24].

2.2 Institutional Collective Action and the Asymmetric Distribution of Sharing Risks

Government data sharing displays the classic characteristics of institutional collective action. The gains generated by sharing—greater administrative efficiency, fewer duplicate submissions, and improved public services—usually accrue to government as a whole and to the public, whereas the costs of data preparation, system modification, security exposure, and accountability are often borne by particular departments. Providing departments must invest resources in data governance, interface construction, and quality maintenance, while the operational benefits of shared data are mainly realized by requesting departments. Requesting departments can reduce repetitive collection but may attribute erroneous administrative outcomes to the data provider, while coordinating authorities can promote systemic collaboration but exercise limited direct control over particular departments' updating and use practices. Because benefits are diffuse and risks concentrated, departments may adopt conservative strategies even when they accept the public value of sharing. Institutional collective action theory shows that interorganizational cooperation may fail not because actors reject the public interest, but because of transaction costs, information asymmetry, responsibility spillovers, and opportunism [12-15]. Without clear standards of responsibility, providing departments cannot predict the risks they will bear after sharing, and requesting departments cannot readily assess accuracy or suitability. Both sides may therefore reduce their exposure by expanding review, restricting interfaces, demanding repeated confirmations, or refusing to share. Overcoming these difficulties requires more than administrative commands or performance targets.

Institutional arrangements must more reasonably align sharing benefits, governance costs, and risk responsibility, while stable application rules, quality statements, purpose limitations, and traceability mechanisms reduce uncertainty in interdepartmental cooperation [10-11,25].

2.3 The Relational and Functional Nature of Administrative Authority over Government Data

In government data sharing, "power" primarily denotes managerial authority and use permissions within the administrative organization, rather than an exclusive property right held by a department. The fact that government data are lawfully collected and generated by a particular department does not give that department the same freedom to decide on access as a private owner disposing of property. The legitimacy of data-management authority derives from statutory functions, and its purpose is to secure lawful provenance, reliability, timely updating, and safe processing. It therefore necessarily carries duties of quality maintenance, cataloguing, and lawful provision. Correspondingly, a requesting department has no abstract or unlimited entitlement to obtain data. Its request must rest on a specific statutory task and remain subject to purpose limitation, data minimization, and security requirements. Guo Wentao argues that the administrative-law basis of public-data sharing must be reconsidered from the perspective of administrative organization and public tasks rather than mechanically importing private-law models of exclusive entitlement; Peng Chun's analysis of the advancement and limits of government data sharing likewise shows that duties to share and restrictions on use are not mutually exclusive but jointly constitute the conditions for lawful data circulation [16,19]. Furthermore, although entities responsible for platform construction, management, and operation generally lack substantive administrative authority, they can in practice influence whether data flow through identity authentication, access configuration, interface design, and default rules, thereby exercising technical control with normative effects. The power structure of digital government thus no longer corresponds entirely to formal authority under traditional administrative organization law; it combines statutory authority with factual control [17,26]. Any allocation of powers and responsibilities must therefore consider both whether an actor has lawful decision-making authority and whether it actually controls the relevant risk, avoiding a situation in which technical actors decide substantive matters in practice yet remain beyond responsibility because they lack formal administrative competence.

2.4 A Task-Control-Causation Framework for Allocating Powers and Responsibilities

The allocation of powers and responsibilities in government data sharing can be analyzed along three dimensions: task, control, and causation. The task dimension asks why an actor is entitled to acquire, manage, or provide data, and therefore uses statutory functions and specific administrative tasks to determine the source and limits of sharing authority. A requesting department may apply only where the data have a substantive connection with its statutory task; a providing department may review a request only by reference to legally defined sharing categories and grounds for restriction; and the coordinating authority's power should be limited to organizational coordination and rule supervision rather than substituting for a business department's substantive administrative judgment. The control dimension asks what duty an actor should bear and assigns conduct-based obligations according to its practical capacity to prevent and manage risks. Source departments control data generation, interpretation, and updating and should therefore bear corresponding quality duties; requesting departments control purposes of use and administrative decisions and should bear duties of purpose management and reasonable verification; platform operators control permissions and transmission and should bear technical-security duties. The causation dimension asks how responsibility should be allocated after an error and determines internal responsibility according to the causal contribution of each actor's conduct, degree of fault, and capacity to avoid harm. These dimensions are not interchangeable: having a statutory task does not imply control over every risk; participation in processing does not automatically confer substantive decision-making authority; and the existence of inaccurate data does not mean that it was the sole cause of the ultimate administrative consequence. This framework also supports a structure of relatively unified external responsibility and layered internal attribution. Externally, the department making an administrative decision or taking administrative action should generally bear responsibility for explanation, correction, and remedies; internally, responsibility should be allocated across data quality, sharing services, technical operation, and administrative use. The framework avoids attributing responsibility solely according to possession, final use, or the location at which harm materializes, and instead aligns the source of authority, control over risk, and responsibility for consequences [8,17].

3 THE STRUCTURE OF POWERS AND RESPONSIBILITIES AMONG THE PRINCIPAL ACTORS IN GOVERNMENT DATA SHARING

3.1 Meta-Governance and Coordinating Responsibility of the Competent Sharing Authority

The competent authority for government data sharing performs a meta-governance function in interorganizational coordination. Its central role is not to manage all government data directly, but to establish the catalogues, standards, procedures, and dispute-resolution mechanisms needed for sustained departmental cooperation. Because sharing involves multiple governmental levels and business systems, an individual provider cannot independently resolve conflicting interdepartmental standards, duplicate construction, or sharing disputes. A coordinating authority with a system-wide perspective is therefore needed to supply institutions, coordinate rules, and supervise performance [7,11,25]. By unifying catalogues and standards, matching supply with demand, coordinating disputes, and conducting

performance evaluation, the authority can reduce interdepartmental transaction costs and resolve complex situations in which the source department is unclear, multiple agencies jointly collect data, or data must flow back across levels of government. Yet coordinating power should not be treated as residual liability for all sharing activities. The authority ordinarily does not participate directly in the creation of original data and lacks the capacity to substantively verify every specialized dataset. Its coordination of application procedures and sharing classifications cannot replace the provider's professional judgment about legal restrictions or the requester's substantive judgment in an administrative matter. The authority should therefore be responsible for organizational failures such as persistent absence of catalogues or rules, delayed dispute resolution, and ineffective supervision, but it should not generally guarantee the accuracy of data or the consequences of uses it cannot control. The responsibilities assigned to competent authorities under the Regulations on Government Data Sharing—overall coordination, catalogue management, dispute handling, and supervision—should be understood as institutional confirmation of this meta-governance role, not as the creation of a central actor with unlimited responsibility for the entire sharing process [23].

3.2 Data Governance and Sharing-Service Responsibilities of Source and Providing Departments

Source departments and data-providing departments may coincide, but their responsibility functions differ. A source department is closest to data formation, business definitions, and update conditions; its principal duty is to ensure that collection has a lawful basis, fields accurately reflect relevant facts, changes are reasonably updated, and error reports are investigated. A providing department stands at the interface through which data move from a management domain into a sharing domain and is primarily responsible for catalogue descriptions, review of requests, version selection, standards conversion, and timely provision. Distinguishing the two prevents all data problems from being subsumed under a vague “provider responsibility”: inaccurate original records and failures to update following changes in substantive rules are source-quality problems, whereas calling the wrong version, failing to provide agreed fields, or delaying a response without justification are defects in sharing services. Data-quality responsibility should not, however, be understood as an absolute guarantee of perfect accuracy. Government data are dynamic, relational, and context-dependent; some are jointly produced by multiple actors, and their meaning may change as administrative rules evolve. Imposing strict liability on a source department for every erroneous consequence in every downstream scenario would exceed its control and could intensify incentives to refuse sharing. A more defensible interpretation treats data-quality responsibility as a process-based governance duty and examines whether the source department has established reasonable mechanisms for collection, validation, updating, objections, and version management, and whether it has adequately disclosed known defects and limits of applicability [7-8]. This process-based conception does not lower quality standards. Where an obvious error could have been discovered and corrected through ordinary performance of duties, data have remained outdated for an extended period, or a department refuses to correct them after verification, the source department should still bear primary responsibility [18,23].

3.3 Application Authority and Administrative-Use Responsibility of Requesting Departments

A requesting department applies for shared data on the basis of statutory functions. Its authority to obtain data is a purpose-limited administrative permission, not comprehensive dominion over the dataset. The request should explain the connection between the data and a particular administrative task and identify the required fields, scope, and duration. Once data are obtained, the department may not change the purpose, widen access, or provide the data onward merely because they have entered its internal system. More importantly, the requesting department must bear independent responsibility for administrative judgments made on the basis of shared data. Government data can reduce repetitive investigation and documentation, but they do not automatically generate a lawful administrative conclusion. The meaning and evidentiary weight of the data, and their relationship to statutory elements, still require substantive assessment by the responsible department. Wang Xixin's work on the rule of law in digital administration demonstrates that data and algorithms significantly empower administrative authority, but technologically mediated fact-finding cannot replace reason-giving, due process, or effective remedies [17]. A requesting department may generally place reasonable reliance on data obtained through proper channels where no obvious anomaly exists, but it cannot avoid verification merely because another department supplied the data. The required degree of verification should correspond to the risk of the decision. Data used for internal statistics or general operational alerts may merit a high degree of reliance; conflicts among data, information evidently beyond its update cycle, or objections raised by affected persons require additional investigation; and a single shared dataset should not ordinarily serve as the sole basis for an adverse decision that may directly produce an administrative penalty, credit sanction, denial of a license, or termination of social-security benefits. The provider's responsibility and the requester's reasonable reliance are not a zero-sum relationship. They should be connected through data-quality statements and risk-based verification duties [16,18,22].

3.4 Technical Control and Safeguarding Responsibility of Platform Operators

A government data-sharing platform is not merely a neutral conduit. Identity authentication, catalogue presentation, application workflows, default settings, field mapping, and permission configuration directly shape the scope and manner of sharing. Zheng Jiasi and Lan Yun note that digital technologies structure the space in which interdepartmental data flow and alter organizational connections and choices of action [26]. Although platform operators generally lack substantive administrative decision-making authority, their control over system architecture

and technical parameters gives them significant factual power. They should therefore bear technical safeguarding responsibilities for account authentication, permission configuration, interface operation, transmission integrity, log retention, and alerts for abnormal calls. Technical control, however, must not turn into an unauthorized substantive decision. Whether particular data are necessary for sharing, whether a statutory restriction applies, and whether the data may support a specific administrative decision are matters for the responsible business department. The platform may translate lawfully approved business rules into technical settings, but it should not generate those rules itself. If a platform implements an erroneous business instruction that it lacks authority and expertise to review, it should not bear responsibility for the substantive judgment; if it expands permissions without authorization, maps fields incorrectly, or fails to retain required logs, it should be responsible for consequences within its technical sphere of control. Outsourcing a platform cannot become a means by which an administrative organ transfers statutory responsibility. The commissioning authority remains responsible for service-provider selection, permission design, and continuing supervision, while the contractor should bear responsibility for processing beyond authorization, unlawful retention, and inadequate security measures [17,20]. Institutional design should accordingly distinguish the formulation of business rules, substantive review, technical configuration, and concrete operation, thereby preventing a reversal in which technical entities decide sharing in fact and business departments merely provide formal approval.

4 MANIFESTATIONS AND CAUSES OF IMBALANCE IN THE ALLOCATION OF POWERS AND RESPONSIBILITIES

4.1 Degeneration of Data-Management Authority into Departmental Possession

Government data sharing first encounters a functional distortion of data-management authority. Through long-term performance of duties, departments develop stable collection channels, business systems, and management rules, and data gradually become resources that support professional authority, operational autonomy, and organizational capacity. In the absence of clear sharing benefits and responsibility safeguards, departments may convert management duties into de facto exclusive control and preserve data boundaries by raising application thresholds, narrowing catalogue coverage, delaying interface access, or repeatedly reviewing necessity. Research shows that local-government data sharing is shaped not only by technical conditions and standards, but also by departmental interests, leadership support, performance incentives, and organizational trust [9-11]. This behavior cannot simply be attributed to an inadequate willingness to share. It reflects stable institutional incentives: the systemic benefits of sharing are difficult to translate into the provider's own performance, while the costs of data preparation, security management, and accountability for errors are borne directly by that department; other departments may expand their operational capacity through shared data, while the provider has limited control over subsequent uses; and data may be misunderstood once detached from their original context. Departmental possession of data thus becomes an organizational strategy for coping with uncertain responsibility. Overcoming this problem requires more than declaring government data to be public in nature. The positive duty to share that accompanies data-management authority must be specified, while quality statements, purpose controls, and layered responsibility reduce downstream risks outside the provider's control. Only when sharing duties and responsibility boundaries are clarified together can data-management authority shift from exclusive control to stewardship [24].

4.2 Conflation of Data-Quality Responsibility and Administrative-Use Responsibility

Government data usually pass through collection, processing, aggregation, conversion, transmission, and use. The data displayed in a requesting department's system may therefore reveal little about where an error originated. A record may be entered by a local unit, aggregated by a higher-level authority, processed by a specialized department, and then supplied through a unified platform. The original data may be accurate while field conversion distorts their meaning; alternatively, a minor defect may exist, but the requester's misinterpretation may be the principal cause of the administrative consequence. Research on data life cycles and cross-domain collaboration shows that responsibility changes as data move and that physical location alone cannot determine attribution. Current rules state that “whoever manages is responsible, and whoever uses is responsible.” This principle is foundational, but it does not resolve the concurrence of management and use responsibilities [23]. If the first clause is read to make the source department responsible for every downstream consequence, the requester's substantive decision risk is shifted to the supply side. If the second is read to make the requester bear all risk of inaccurate content, the source department's incentive to improve quality is weakened. Attribution must further consider whether an error lay within an actor's sphere of control, whether the requester could have discovered the anomaly through ordinary care, what role the erroneous data played in the decision, and whether another actor altered the original information. Data-quality responsibility and administrative-use responsibility are not mutually exclusive; both may coexist in the same causal chain. The key is to distinguish the respective causal contribution of data defects, defects in sharing services, technical defects, and defects in administrative judgment [12-13,18].

4.3 Interpenetration of Substantive Review Authority and Platform-Based Technical Power

As government data sharing becomes fully platform-based, applications, reviews, and authorizations once performed by administrators are increasingly translated into standardized digital workflows. Mandatory fields, automated checks,

default authorization scopes, and interface rules structure administrative action and can improve efficiency, but technical configuration may also embed value judgments that should be made by substantive departments. A system that presumes automatic approval for a category of data already influences the review decision; a platform that converts data from different departments into uniform fields may alter their meaning in the original business context; and an algorithm that configures permissions by request type may broaden access without substantive review. Research on collaborative e-government shows that technical systems and organizational institutions are intertwined: platform architecture can entrench existing power relations and create new control structures [14,26]. The difficulty is that platform operators often lack substantive administrative authority but control technical nodes that determine whether data flow, while business departments possess formal review authority but may lose effective judgment by relying on system defaults. When errors occur, business departments may claim that the system acted automatically, while technical units may claim merely to have executed instructions, producing a gap between factual control and formal responsibility. The rule of law in digital administration requires technical rules to be traceable to lawful business authorization and requires identifiable records of those who participate in rule design, parameter setting, and permission adjustment [17].

4.4 Imbalanced Accountability Incentives Caused by Conflating External Responsibility and Internal Attribution

Once shared data are used in an administrative decision that affects the rights or interests of a citizen or legal person, the affected party will ordinarily perceive only the requesting department that made the decision. It cannot know which department generated the data, through which platform they travelled, or at what point an error arose. Requiring the individual to identify the "true" responsible actor among multiple departments would increase the cost of remedies and might allow the requesting department to refuse correction because another agency supplied the data, while the source department refuses action because it did not make the decision. Conflating external responsibility with internal attribution therefore undermines the identifiability of administrative accountability. At the same time, current accountability practices more readily identify data leaks, unauthorized access, and unlawful provision because they produce visible events, but are less able to detect the diffuse harms caused by refusal to share, delayed responses, incomplete catalogues, or low-quality provision. Dawes's analysis of information-sharing risks shows that organizations may reduce cooperation when expected risks exceed direct benefits; institutional collective action theory similarly demonstrates that passive cooperation may be organizationally rational where individual actors bear costs and responsibility while benefits spill over to others [12,15]. Strict accountability for post-sharing security incidents, without comparable scrutiny of unjustified non-sharing, creates an incentive structure in which not sharing is safer than sharing. Conversely, evaluating performance solely by call volume or number of interfaces can encourage formalistic sharing that disregards purpose limits and data quality. The allocation of powers and responsibilities must simultaneously address how affected parties obtain effective remedies, how government traces internal errors, and how departments develop stable expectations for cooperation. Responsibility cannot be reduced to personnel sanctions after a security event [16,20].

5 IMPROVING THE ALLOCATION OF POWERS AND RESPONSIBILITIES IN GOVERNMENT DATA SHARING

5.1 Reconstructing Data-Management Authority around Public Tasks

Administrative authority over government data should move from a logic of departmental possession to one centered on public tasks. A source department holds management authority because it performs the relevant administrative task and possesses professional capacity to maintain the data, not because generation within its system confers an exclusive power of disposition. Data-management authority should be understood as a functional authority carrying positive obligations. It includes lawful access control, quality maintenance, and security, but also cataloguing, reasonable explanation of data conditions, and provision to legitimate requests made for statutory purposes. The requesting department's application authority should likewise be bounded by public tasks. A bare assertion of "work needs" is insufficient; the request should identify the statutory function, operational scenario, necessary fields, and period of use. If a providing department refuses to share, it should explain the specific facts and legal basis and why a narrower scope, de-identification, or additional security condition cannot enable lawful sharing. Reason-giving allows the requester to decide whether to object and enables the coordinating authority to act on reviewable facts and legal grounds [16,19]. Dynamic catalogues may disclose categories of conditional and non-shareable data and their application requirements, but abstract invocations of security or personal information should not become permanent grounds for refusal. The competent sharing authority should primarily examine the relationship between the request and the statutory task, the legal basis for refusal, and procedural reasonableness, without replacing the business department in deciding the underlying administrative matter. This creates a structure in which source departments manage lawfully, requesting departments apply according to function, providing departments review on stated grounds, and coordinating authorities intervene proportionately. Sharing then no longer depends on ad hoc administrative bargaining, while requests do not become open-ended claims to data [23].

5.2 Establishing a Layered Responsibility System Based on Task, Control, and Causation

Responsibility should be layered according to the point at which a data-related risk arises. Source departments should bear data-quality responsibility for provenance, original content, business definitions, update rules, and verification and correction, but the central inquiry should be whether reasonable governance duties were performed rather than whether every downstream outcome was accurate. Providing departments should bear sharing-service responsibility for catalogue classification, response to applications, data versions, interface content, and quality statements. Platform operators should bear technical-operation responsibility for identity authentication, permission configuration, field mapping, transmission, log retention, and abnormal-use alerts. Requesting departments should bear responsibility for necessity of the application, scope and purpose of use, access management, reasonable verification, and administrative decisions based on the data. Attribution should first determine, by reference to the statutory task, whether the actor had authority to make the decision; second, assess whether actual control enabled the actor to prevent the error; and third, evaluate the causal contribution of the breach to the outcome [18]. For example, where a source department fails to update data as required and directly causes an erroneous determination that the requester had no reasonable means to detect, the source department should bear primary internal responsibility. Where data clearly state their update time and limits of applicability, but the requester uses them in a high-risk decision outside that scope, the requester should bear primary responsibility. Where incorrect field mapping by the platform changes the meaning of data and the business department uses them through ordinary procedures without a feasible means of detecting the error, technical responsibility should be primary. Where data are defective and the requester also fails to investigate an obvious inconsistency, shared responsibility should be allocated according to each actor's causal contribution. This layered approach translates the slogans “whoever manages is responsible” and “whoever uses is responsible” into operational standards.

5.3 Linking Unified External Responsibility with Layered Internal Attribution

As a general rule, where a requesting department makes an administrative decision based on shared data, the department that made the decision should bear external responsibility for explanation, correction, and remedies. The affected party should not be required to reconstruct the entire chain of data generation, provision, transmission, and use, nor should internal governmental divisions impose additional remedial costs. If the requesting department discovers that its decision may rest on erroneous data, it should investigate proactively and, as required by law, suspend enforcement, modify, revoke, or remake the decision; it should not merely direct the affected person to seek correction from the source department. Unified external responsibility does not mean that the requesting department bears all ultimate internal responsibility or that other actors are relieved of their duties. After the decision is corrected, call logs, data versions, review records, and quality statements should be used to identify the defective stage, and internal responsibility should then be allocated among the source department, providing department, platform operator, and requesting department according to fault and causation [17,22]. Where a platform operator or another department independently engages in unauthorized processing, disclosure of personal information, or other unlawful conduct, it should bear responsibility for its own act rather than having that responsibility absorbed by the decision-making department. Distinguishing the external responsible actor for the administrative act from the internal responsible actors along the data chain both protects timely remedies and prevents the requesting department from bearing other actors' risks indefinitely under the rule of unified external responsibility. Internal attribution should primarily correct institutional defects, clarify organizational responsibility, and prevent recurrence; interdepartmental disputes must not delay external correction.

5.4 Establishing Whole-Process Responsibility Matrices and Risk-Based Verification

A matrix of powers and responsibilities for government data sharing should do more than summarize departmental functions; it should correspond to the data life cycle and to concrete processing acts. At the cataloguing stage, it should identify responsibility for compiling catalogues, conducting substantive review, and updating dynamically. At the application stage, it should record the requesting department's statutory basis, data scope, use scenario, and period. At the review stage, it should record the provider's reasons, conditions, and grounds for refusal. At the provision and transmission stages, it should preserve data versions, quality status, interface parameters, permission changes, and anomalies. At the use stage, it should record authorized personnel, the relevant administrative matter, whether an external decision was produced, and whether additional verification occurred. At the verification and correction stage, it should record error reports, corrections, the range of historical calls, and linked notifications. At the retention and deletion stage, it should confirm whether data were deleted on schedule or lawfully transferred to another management status. Life-cycle research demonstrates that points of responsibility transfer can be identified only by combining changes in data status with actor conduct. Data-quality metadata and version management should also accompany shared data, including source, time of formation, most recent update, scope of applicability, known defects, and verification status, so that requesting departments do not treat every shared dataset as possessing equal evidentiary weight. Verification duties should be graded according to the consequences of the administrative action. Ordinary internal analysis may reasonably rely on shared data; data conflicts or material beyond its update cycle require supplementary verification; and major adverse decisions should involve cross-source comparison, human review, and an opportunity for the affected person to explain and correct the record. Sharing involving personal information must

also satisfy lawfulness, propriety, necessity, and security, but personal-information protection should not be abstracted into a ground for refusing all sharing. It should be implemented through field minimization, access controls, and use-scenario restrictions [20].

5.5 Building Incentives and Constraints that Address Both Non-Sharing and Unlawful Use

An effective responsibility regime must constrain over-sharing, unlawful use, and passive non-sharing at the same time. Evaluation of source and providing departments should include catalogue completeness, timely updating, response periods, handling of verification requests, data quality, and unjustified refusal. Evaluation of requesting departments should focus on whether the requested scope was necessary, whether data were actually used for statutory tasks, whether access permissions were appropriate, and whether purpose-incompatible uses occurred. Platform operators should be assessed by accuracy of permission configuration, capacity to detect anomalies, completeness of logs, and response to security incidents. The emphasis should shift from the number of interfaces and calls to the actual contribution of sharing to interdepartmental performance, reductions in materials required from businesses and citizens, and the quality of administrative decisions, avoiding low-value interfaces or meaningless calls created merely to satisfy quantitative indicators [10,25]. At the same time, due-performance assessment should correspond to the actor's capacity to control risk. A providing department that has completed data validation according to applicable standards, issued appropriate quality statements, and adopted reasonable safeguards should not bear unlimited responsibility for unforeseeable unlawful use by a requester. Where a requesting department has completed the verification required for the relevant risk level but still suffers consequences from a concealed source error, its performance of the duty of care should be considered in internal attribution. Due-performance assessment, however, must not become a general exemption. It can distinguish degrees of responsibility but cannot protect an actor that intentionally conceals defects, refuses without justification to update data, or ignores obvious risks. Bringing passive non-sharing, low-quality sharing, use beyond scope, and technical dereliction within the same supervisory framework—and giving actors that perform lawfully and take reasonable measures stable expectations—can reduce the cooperation difficulties created by the asymmetry between systemic benefits and departmental risks [12,15].

6 CONCLUSION

Digital government development requires data to cross traditional organizational boundaries, while administrative authority must still be allocated by statutory function. This tension means that government data sharing cannot depend solely on platform construction or general commands to share. Its essence is to reconnect data-management authority, the authority to request sharing, technical control, and administrative responsibility without abolishing departmental specialization. Management by a source department does not confer an exclusive right of possession; lawful acquisition by a requesting department does not remove duties of purpose control and administrative judgment; the coordinating authority should promote collaboration but cannot serve as the guarantor of every risk; and platform operators exercise important technical control but may not replace substantive administrative decisions through technical configuration.

The allocation of powers and responsibilities in government data sharing should use statutory tasks to define jurisdictional boundaries, actual capacity for control to assign conduct-based duties, and causation and degree of fault to allocate internal responsibility. Within this framework, data-quality responsibility, sharing-service responsibility, technical-operation responsibility, and administrative-use responsibility are distinct but together form a complete chain of responsibility. For administrative consequences arising from shared data, the department making the decision should generally bear unified external responsibility for correction and remedies, followed by internal attribution according to the stage at which the error arose. Future institutional development should focus not on multiplying general duties to share, but on converting abstract principles into standards that are determinable, enforceable, and traceable through quality statements, risk-based verification, whole-process records, and two-way accountability. Only when management authority carries a duty to share, data use carries administrative responsibility, technical control carries security responsibility, and both non-sharing and improper use are corrected can government data sharing reconcile whole-of-government coordination, departmental boundaries of competence, and the protection of individual rights.

COMPETING INTERESTS

The author has no relevant financial or non-financial interests to disclose.

REFERENCES

[1] State Council of the People’s Republic of China. Guiding Opinions on Strengthening the Development of Digital Government: State Council Document No. 14[2022]. 2022.
[2] Zhang C F, Xie K K. Government Transformation and Digital Government in the Digital Age. Administrative Tribune, 2020, 27(6): 34-41.
[3] Huang H. Digital Government: Policy, Characteristics, and Concept. Governance Studies, 2020, 36(3): 6-15.
[4] Huang H. Governing “Data Flows”: Theoretical Evolution and a Framework for Government Data Governance. Nanjing Journal of Social Sciences, 2018(2): 53-62.

[5] Xu X L, Ming C H, Chen T. Data Sharing in Government Services in the Context of Digital Government. Administrative Tribune, 2018, 25(1): 50-59.
[6] Li C Z, Huang H. Factors Influencing Data Sharing by Chinese Local Governments. Chinese Public Administration, 2019(8): 47-54.
[7] Yuan G, Wen S J, Zhao J J, et al. Integration and Sharing of Government Data Resources: Demand, Constraints, and Key Pathways. E-Government, 2020(10): 109-116.
[8] Dawes S S. Interagency Information Sharing: Expected Benefits, Manageable Risks. Journal of Policy Analysis and Management, 1996, 15(3): 377-394. DOI: 10.1002/(SICI)1520-6688(199622)15:3<377::AID-PAM3>3.0.CO;2-F.
[9] Yang T M, Maxwell T A. Information-Sharing in Public Organizations: A Literature Review of Interpersonal, Intra-Organizational and Inter-Organizational Success Factors. Government Information Quarterly, 2011, 28(2): 164-175. DOI: 10.1016/j.giq.2010.06.008.
[10] Gil-Garcia J R, Chengalur-Smith I, Duchessi P. Collaborative E-Government: Impediments and Benefits of Information-Sharing Projects in the Public Sector. European Journal of Information Systems, 2007, 16(2): 121-133. DOI: 10.1057/palgrave.ejis.3000673.
[11] Feiock R C. The Institutional Collective Action Framework. Policy Studies Journal, 2013, 41(3): 397-425.
[12] Peng C. Advancing Government Data Sharing and Defining Its Limits. Jiaotong University Law Review, 2023(6): 63-77.
[13] Wang X X. Data-Based Governance and the Rule of Law: Legal Constraints on Digital Administration. Journal of Renmin University of China, 2022, 36(6): 17-34.
[14] Wang X X. Risks of Government Data Aggregation and Their Legal Control. Journal of East China University of Political Science and Law, 2024, 27(3): 23-38.
[15] Guo W T. A New Administrative-Law Foundation for Public Data Sharing. Northern Legal Science, 2023, 17(6): 98-110.
[16] Su Y. Legal and Institutional Safeguards for Government Data Security. Journal of Soochow University (Law Edition), 2023, 10(4): 27-42.
[17] Pan X J, Nie J Q. Justifying the Legal Principles of Data Sharing. Academic Exploration, 2023(11): 94-101.
[18] Liu Q. Integrating Digitization and the Rule of Law in Digital Government Development. Contemporary Law Review, 2023, 37(6): 15-25.
[19] State Council of the People's Republic of China. Regulations on Government Data Sharing: State Council Decree No. 809. 2025.
[20] Tang Y Q. From Fragmentation to Holism: Governance of Data in Grassroots Government Services. Administrative Tribune, 2022, 28(1): 87-93.
[21] An X M, Guo M J, Wei W. Capacity Building for Collaborative Innovation Communities in Government Information-System Integration and Sharing Projects. Information Studies: Theory & Application, 2019, 42(4): 76-82.
[22] Zheng J S, Lan Y. Shaping the Space of Data Flows: A New Technical Mechanism for Interdepartmental Government Data Sharing. Journal of South China Normal University (Social Science Edition), 2022(5): 43-55.
[23] Li Y, Cao H J. Cross-Domain Collaborative Data Governance in Government from a Data Life-Cycle Perspective and Its Operational Logic. Journal of Northeastern University (Social Science), 2020, 22(3): 56-63.
[24] Wang X, Zheng L. "Public" Data Governance: Scope, Objectives, and a Content Framework. E-Government, 2024(1): 2-9.
[25] Standing Committee of the National People's Congress. Data Security Law of the People's Republic of China. 2021.
[26] Standing Committee of the National People's Congress. Personal Information Protection Law of the People's Republic of China. 2021.