ISSN: 2688-9323

Construction of Digital Audit Supervision Mechanism from the Perspective of Soft Corruption Governance

Jie Lyu*, Yuting Wang

School of Law, Nanjing Audit University, Nanjing 211815, China

Abstract

Currently, the form of power corruption is evolving from overt economic corruption to implicit "soft corruption". Traditional fiscal and financial compliance-oriented audit supervision faces challenges such as unclear targets, difficult evidence preservation, and lack of standards. In the digital age, the entire process of public power operation can form traceable and computable supervision objects within information systems, providing opportunities for the governance of "soft corruption". This paper aims to establish a digital audit supervision mechanism. At the same time, standardize data collection and usage rules, safeguard data subjects' remedies rights, and guarantee the legal validity of audit results.

Keywords

Corruption Governance; National Audit Supervision; Digital Audit; Audit Rule of Law.

1. Introduction

Since the 18th National Congress of the Communist Party of China, the anti-corruption struggle has achieved an overwhelming victory and been comprehensively consolidated. However, "soft corruption" characterized by laziness, negligence, and selective law enforcement has gradually become prominent. The non-monetization and behavioral characteristics of "soft corruption" pose challenges to traditional compliance-oriented national audits in identifying issues, preserving evidence, and determining responsibility. Currently, big data mining and artificial intelligence analysis provide new technological paths for digital audit supervision throughout the entire process of power operation. However, technology empowering supervision itself brings profound legal questions. Using digital technology to strengthen audit supervision must carefully define the legal boundaries of data collection and processing to ensure the transparency, fairness, and legality of algorithmic decisions. Under the new situation of anti-corruption, this paper aims to explore the construction of a national audit anti-corruption mechanism that combines technical effectiveness with rule of law connotations, providing theoretical reference for promoting the in-depth development of the anti-corruption struggle.

2. Jurisprudential Basis of Digital Supervision Mechanism for National Audit

2.1. Integration of National Audit and Digital Audit

The theoretical cognition of national audit has deepened from "audit supervision" to "immune system" and then to "national governance". In this process, the role of audit has moved from a static economic supervisor to a dynamic immune system, eventually being established as an important component of national governance that combines strategic and systemic functions [1] . Digital audit is a new audit model that has emerged with the digital transformation of national governance. Its core lies in using information technologies such as big data and artificial intelligence to collect, analyze, and supervise behavioral data generated during the

ISSN: 2688-9323

operation of public power, in order to achieve precise profiling, risk warning, and effectiveness assessment of audit subjects. From sampling inspections focused on financial accounts to a panoramic review of full-process data from power actions, from compliance testing relying on manual experience to algorithmic model-based correlation mining and anomaly detection, and from periodic static supervision to continuous dynamic monitoring, this transformation not only broadens and deepens national audit supervision but also reshapes the underlying logic of audit work through technological empowerment, transforming the symptom-relief function of post-event audit into the fundamental function of pre-event audit.

2.2. Typological Analysis of "Soft Corruption" Behaviors

The essence of "soft corruption" is the concentrated manifestation of the distorted view of power and the lack of responsibility awareness. Its harm is not direct economic corruption, but inaction in diligent governance, a hidden form of power distortion. According to the behavioral pattern and the nature of harm, typological analysis can be conducted.

The first is "lazy corruption", manifested as public officials failing to perform or delaying performance without legitimate reasons, or failing to adequately perform statutory duties. For example, they deliberately delay legitimate applications or delay legitimate applications beyond the statutory deadline. This kind of administrative inertia essentially undermines the function of public services and erodes the credibility of government implementation.

The second is "abuse of power corruption", whose core lies in the abuse of discretionary power. Actions may formally have legal grounds but actually violate the principles of legal purpose and rationality, such as different penalties for the same case in administrative law enforcement and excessive severity in policy implementation. Such actions distort the original intent of policies and undermine market fairness and social justice.

The third is "evasive corruption", which uses formalism to cover up substantive injustice, such as theatrical meetings and templated reports creating the illusion of performing duties, or placing matters on interdepartmental official travel to evade substantive responsibility, resulting in the waste of administrative resources and the quiet erosion of public interests under compliance procedures.

2.3. Legal Legitimacy of Digital Audit as an Anti-corruption Tool

The legal basis of digital audit orginates from the modern national governance principle of "supervising public authority and fulfilling public fiduciary responsibility". Authorized by the Constitution and laws, digital audit supervision power operates within a strict procedural justice framework to ensure its legitimacy. By enhancing supervisory effectiveness, enhancing objectivity and fairness, and safeguarding the public's right to know, it demonstrates its great tool rationality and social legitimacy.

Digital audit is an institutional innovation of self-supervision and self-regulation by administrative agencies. By establishing a normalized digital audit mechanism, continuous supervision of administrative processes can be achieved, compensating for the shortcomings of traditional post-event supervision. This supervision mode aligns with the requirements of the "State Council's Opinions on Strengthening the Construction of a Law-Based Government" to "strengthen the restriction and supervision of administrative power". In addition, digital audit also reflects the application of the preventive principle of "combining punishment with education" in the field of audit supervision. Through big data analysis and technical early warning, abnormal situations in power operations can be detected in time, shifting from post-event accountability to proactive prevention.

ISSN: 2688-9323

3. Construction of a Digital Audit Supervision Mechanism to Address the Governance of "Soft Corruption"

3.1. Digital Analysis of "Soft Corruption"

The key to addressing "soft corruption" lies in precise detection and timely accountability. To this end, a "top-down, internal and external collaborative" supervision system must be established [2] . Based on digital audit, "soft corruption" can be divided into quantifiable behavioral patterns, including non-action and slow action, abuse of discretion, formalism and bureaucratism, benefit transfer, and wastefulness. For these types, audit supervision should follow the principles of "data-driven, risk-oriented, and continuous monitoring" to build a closed-loop management system.

Firstly, the data collection process must strictly comply with the provisions of Article 6 of the Personal Information Protection Law (2021), following the principle of minimum necessity. Information involving personal privacy should undergo de-identification processing. Establish a data grading and categorization management system. According to Article 21 of the Data Security Law (2021), power-related behavioral data is divided into general data, important data, and core data, implementing differentiated management measures, with the goal of building a comprehensive "soft corruption" audit database.

Among them, general data refers to data generated during the exercise of power, which does not involve sensitive information and may cause minor impact or inconvenience if leaked. Such as non-confidential meeting notices, times, and locations, public service procedures and regulatory texts, and employees' public identity information. Important data refers to data that, once leaked, may directly harm the legitimate rights and interests of specific individuals, or cause certain damage to the organization's internal management order and credibility. For example, employee ID numbers, home addresses, contact information, personnel files, precise attendance data, undisclosed internal rules and regulations, work plans, original performance assessment data, internal meeting minutes, preliminary opinions of government approval, non-final decision-making process drafts, preliminary clues of internal audits, intermediary results of abnormal behavior detection, etc. Core data refers to data that relates to an organization's core interests and critical security, and if leaked, it could seriously endanger national security, public interests, organizational survival, or lead to systematic audit failures. For example, undisclosed discussions and decision records of major strategic decisions, mergers and acquisitions, personnel appointments and removals, sources of leads, investigative methods, evidence collection processes, and data for discipline inspection, supervision, and internal anti-corruption investigations, core algorithms, rule engines, risk weighting parameters, and correlation graph analysis models for "soft corruption" audit supervision models.

Secondly, the crucial step in converting raw data into recognizable features by the model is cleaning and standardizing the data, such as standardizing time, units, personnel codes, etc. Extracting commonalities from different data sources can improve the economic efficiency of data analysis and achieve fairness.

Thirdly, data analysis comprehensively applies multiple algorithmic models to form a digital mirror of "soft corruption" risks. Establish rule models to identify clearly violating behaviors, such as setting "average spending per official reception must not exceed X yuan", with the system automatically marking records that exceed the limit; establish anomaly detection models to detect behaviors deviating from normal patterns in massive data, establish an Isolation Forest [3] to quickly identify anomalies in high-dimensional data, such as an employee's reimbursement frequency that is significantly higher than that of their colleagues, abnormal approval durations, etc.

ISSN: 2688-9323

Finally, converting model results into audit information and evidence is key to the application and optimization of digital audit. By integrating data into the audit supervision platform, newly generated power behavior data can be scored in real or near real-time, with different levels of warning thresholds set. The platform automatically pushes warning information and generates intelligent audit reports.

3.2. Monitoring Function of Digital Audit on Fiduciary Responsibility for "Soft Corruption" Behaviors

The fiduciary responsibility monitoring function of digital audit for "soft corruption" behaviors has fundamentally reshaped the traditional responsibility supervision model, shifting from post-event investigation to fully embedded precision monitoring throughout the process. Traditional fiduciary duty supervision mainly focuses on whether there are violations of explicit provisions, known as "hard corruption", while digital audit can penetrate superficial compliance to assess the efficiency, effectiveness, and fairness of power exercise, that is, whether substantive fiduciary duties have been truly fulfilled.

The evolution of its core functions is reflected in the following four aspects, which are highly aligned with the AOM model [4] :

1) Break down information barriers and foster a transparent and trustworthy governance environment. From information asymmetry to data pivot, traditional "soft corruption" relies on information opacity. Digital audit has established a trust environment characterized by high transparency and traceability through cross-departmental data connectivity. The decision-making process, policy implementation trajectories, and the flow of public resources of public servants are all recorded in a data-driven manner. For example, the duration circulation, reasons for rejection, and modification records of a task have become analyzable, making negative "soft corruption" such as inaction or slow action nowhere to hide.

2) Provide opportunities for precise supervision, ensuring that government data is well-documented and verifiable. Through big data models, massive amounts of official behavior data can be scanned to automatically identify abnormal patterns, such as unusually dense interaction circles of specific personnel and resource allocations during unconventional times. Digital audit has changed the passive situation of relying on whistleblowing and accidental discovery in the past, enabling supervisors to proactively identify clues of "soft corruption". Supervision is no longer about aimless spot-checking, but about precise guidance driven based on data-driven analysis.

3) Strengthen the ability to comply with regulations and guide individuals to proactively avoid of responsibility for "soft corruption". A well-designed digital audit system is not only a supervisory tool but also a capability support system. Through clear process guidance, automatic compliance verification, and risk warnings, it helps officials clearly understand what constitutes compliance and what are the red lines. To prove their innocence, officials are more motivated to proactively adopt standardized and transparent behaviors, thereby fundamentally curbing the occurrence of "soft corruption".

4) Form a virtuous cycle of motivation, so that both laziness and disorderly behavior will be made to pay a price. Digital audit has reshaped the costs and benefits of behavior through continuous data recording and analysis. Inefficient and shirking behavior patterns will be identified and warned by the system, attempting to establish private domains and obtain gray benefits through "soft corruption", which faces extremely high exposure risks due to data correlation analysis. The ultimate trigger mechanism is legal transformation—turning data clues into formal investigations and accountability. This makes it possible and inevitable to hold accountable those who engage in "soft corruption" behaviors, which were previously difficult to trace.

ISSN: 2688-9323

4. Legal Improvement for the Construction of Digital Audit Supervision Mechanism

4.1. Standardize Data Collection and Usage Rules

Firstly, establish a classified and hierarchical system for data rights protection (see Table 1). On the basis of clarifying personality rights as the core of personal information protection, property rights attributes are introduced as a supplement, constructing a dual rights protection model. Specific supervisory agencies should be legally authorized to carry out data collection and processing for anti-corruption purposes, while strictly defining the boundaries of their powers. Based on the risk level of positions and the severity of problem clues, differentiated data collection standards should be established. For high-risk positions, correspondingly intense data monitoring measures can be taken, while for low-risk positions, high-intensity monitoring is prohibited, ensuring that data collection methods are commensurate with regulatory objectives.

Table 1. Classification and Grading System Table for Data Rights Protection

Job Level Risk	Problem Clue Severity	Data Collection Intensity Level	Measures That Can Be Taken
Low risk	No specific clues	No monitoring	In principle, no targeted data collection or monitoring is conducted.
	Low degree	General monitoring	Only publicly available government data can be queried and monitored.
	Moderate degree	Authorized monitoring	Only with written approval and authorization can targeted queries and monitors certain internal government data.
	High degree	Comprehensive monitoring	Comprehensive and in-depth monitoring of their administrative behavior after high-level approval.
Medium risk	No specific clues	General monitoring	Regular monitoring can only query and monitor publicly available government data.
	Low degree	Restricted monitoring	Preliminary verification can retrieve internal government data and asset disclosure information related to the clues.
	Moderate degree	Authorized monitoring	Focused investigations, after authorization and approval, can investigate and monitor government data and sensitive personal information.
	High degree	Comprehensive monitoring	Comprehensive and in-depth monitoring of their administrative behavior after high-level approval.
High risk	No specific clues	Restricted monitoring	Preventive supervision involves conducting compliance data audits on key government data.
	Low degree	Authorized monitoring	After authorization and approval, their financial status and social network will be automatically verified.
	Moderate degree	Comprehensive monitoring	Focus on in-depth auditing in accordance with the law, and utilize various detection methods for comprehensive audit monitoring.
	High degree	Comprehensive monitoring	A special task force has been established to conduct comprehensive and in-depth data auditing and monitoring, using all compliant measures in accordance with the law.

ISSN: 2688-9323

Secondly, strengthen the protection of sensitive personal information (See Table 2). Classify personal information into general data, important data, and core data, with pre-procedure for manual review to avoid automatically collecting and using such information through technical means. Meanwhile, improve rights remedy channels to ensure that information subjects can obtain effective legal remedies when their rights are damaged.

Table 2. Strengthening the Protection of Sensitive Personal Information Form

Information level	Pre-use review procedure	Channels for remedying information subject rights
General data	Automated processing	The information subject has the right to know who is using the information; when errors are found in the information, they can submit an application, and have the rights to inquire, correct, and delete.
Key data	Manual Pre-Review (Approval Required)	If the information subject has objections to the use of the information, they can lodge an appeal or complaint.
Core data	High-level manual review (requires forming a committee including legal and technical experts)	Judicial remedies and state compensation

4.2. Guarantee the Relief Rights of Data Subjects

The legislative purpose clause clearly states that the purpose of digital audit technology is to "protect cadres, prevent risks, and enhance governance effectiveness". The analysis results of the data model are only used as early warning tools to identify "soft corruption" risks and reference for assisting decision-making, and cannot be used as the sole basis for evaluating cadres.

Introduce a data supervision procedure system. Supervisory authorities should apply for permission from an independent judicial or quasi-judicial body before conducting large-scale or sensitive data collection to demonstrate its necessity.

A mechanism for initiating investigations with manual review prior to manual review should be established. The output results of the model must not be used as legal evidence or clues for initiating an investigation procedure. It must be evaluated by a manual review committee, which should make a reasonable judgment on the early warning clues based on the cadres' consistent performance and specific work situation to ensure the prudence of the investigation initiation.

Guarantee cadres' right to interpret and appeal. Any cadre who is adversely affected by the model warning has the right to receive a non-technical explanation which is understandable to an ordinary person, and the right to raise objections to an independent appeal committee.

4.3. Ensure the Legal Validity of Audit Results

The data analysis results, risk scores, or early warning information generated through digital audit models and other algorithmic tools do not have independent legal evidentiary effect. It should be clearly defined in relevant laws and regulations as clues for problem discovery and as references for assisting decision-making, rather than replacing statutory investigation procedures or substantive judgments.

Firstly, the supervisory authorities must initiate and complete independent and comprehensive investigation and verification in accordance with the authority and procedures stipulated by the Oversight Law of the People's Republic of China, the Criminal Procedure Law of the People's Republic of China, the Rules for the Supervision and Discipline Enforcement Work of the Discipline Inspection Organs of the Communist Party of China, and other relevant laws and

ISSN: 2688-9323

regulations, as well as intra-Party regulations. Secondly, the verdict must be based on the types of statutory evidence obtained through legal means. Supervisory authorities should strictly use traditional investigative methods to preserve and transform evidence based on the clues provided by the model.

5. Conclusion

This study focuses on the legal mechanisms for digital audit supervision of "soft corruption", demonstrates the legitimacy of digital audit supervision from a legal perspective, and typifies "soft corruption" behaviors to construct an operablee supervisory framework. On this basis, an audit supervision model featuring "data-driven, risk-oriented, and continuous monitoring" has been designed, achieving precise early warning through data classification and grading. To address the operation of the digital audit supervision mechanism, we should improve data classification and authorization rules, establish auxiliary positioning and manual review mechanisms for audit results, and strictly regulate the transformation of clues and the use of evidence.

References

[1] Tan, J. S., & Song, S. L. (2012). National audit and national governance: Theoretical basis and realization path. Auditing Research, (2), 3–8.

[2] Li, H. Q. (2018, November 20). To achieve an overwhelming victory, efforts should be made to govern "soft corruption". Procuratorial Daily, p. 008.

[3] Cai, L. J., Li, X., Wang, Z. Y., & Chen, Z. H. (2025). Research on active early warning of audit data anomalies based on improved isolation forest algorithm. Information Technology and Informatization, (3), 131–134.

[4] Xie, P. B., Xie, Q. H., Wang, J. F., & Qin, Y. M. (2024). The underlying logic and realization path of digital audit: From the perspective of national audit. Finance and Accounting Monthly, 45(1), 72–78.