



Enhancing citizens' social supervision in anti-corruption through digital platforms in Vietnam: Legal framework, comparative perspectives and reform recommendations

Nguyen Anh Tung

Faculty of Criminal Law, Hanoi Law University, Vietnam

DOI: <https://doi.org/10.66856/ijl.2026.12.4.12338>

Abstract

The digital transformation of public governance has created new opportunities for strengthening citizens' social supervision in anti-corruption, yet the effectiveness of digital platforms depends on the adequacy of the legal and institutional framework governing citizen participation, data sharing, and information protection. This article examines whether and how digital platforms can improve social supervision and contribute to more proactive and accountable anti-corruption governance in Vietnam. It argues that digital reporting mechanisms alone cannot ensure effective oversight unless they are supported by interoperable public databases, meaningful access to open data, reliable mechanisms for verifying electronic information, and adequate safeguards for citizens who report suspected corruption. The study employs doctrinal legal analysis and a comparative approach, examining Vietnam's legal framework and existing digital supervision mechanisms alongside the experiences of Estonia and China. The analysis identifies four major constraints in Vietnam: fragmented administrative databases, limited access to machine-readable public information, difficulties integrating citizen-generated information into asset and income verification, and risks associated with disclosing reporters' identities. The comparative findings indicate that Estonia offers relevant lessons on open data, interoperability, and data traceability, while China provides insights into digital reporting mechanisms, electronic evidence, and data-supported supervision. However, both approaches also highlight the need to balance technological efficiency with privacy protection, institutional accountability, and human oversight. The article recommends strengthening legal safeguards for digital whistleblowers, improving lawful data interoperability, expanding open data in corruption-prone sectors, and ensuring that algorithmic risk assessments remain subject to independent human verification. It concludes that effective digital social supervision requires an integrated, rights-protective legal and institutional framework that connects citizen participation with transparent, verifiable, and accountable anti-corruption processes.

Keywords: Social supervision, anti-corruption, digital platforms, big data, open data, electronic evidence, whistleblower protection, Vietnam

Introduction

Digital transformation is reshaping how citizens participate in public governance and exercise social supervision over the use of public power. In anti-corruption, digital platforms create opportunities for citizens to report suspected misconduct, provide supporting information, and help identify corruption risks early. However, the availability of digital reporting channels does not necessarily translate into effective social supervision. Their effectiveness depends on whether citizens can lawfully verify and use information, whether relevant public databases can be securely interconnected, whether public information is sufficiently accessible, and whether individuals who provide information are adequately protected against unauthorized disclosure and retaliation. In Vietnam, the development of digital government and the emergence of platforms such as VNeID provide an important foundation for expanding citizen participation, while also raising questions concerning the relationship between digital reporting, data governance, electronic evidence, and existing mechanisms for preventing and detecting corruption. Although scholars have increasingly examined the application of digital technologies and Big Data to anti-corruption, the legal and institutional conditions under which digital citizen participation can become effective, accountable, and rights-protective social supervision require further examination. Against this background, this article examines Vietnam's legal framework and existing digital supervision mechanisms, identifies the principal legal and institutional

constraints, and draws comparative insights from Estonia and China. Using doctrinal and comparative legal analysis, it examines how open data, interoperability, digital reporting, data traceability, and safeguards for information providers can inform a more coherent framework in Vietnam. The article argues that strengthening digital social supervision requires not merely expanding reporting platforms, but integrating citizen participation with lawful data sharing, accessible public information, reliable verification procedures, and effective protection of individual rights. On this basis, it proposes legal and institutional reforms to make digital technologies a means of strengthening transparency, public accountability, and anti-corruption governance, rather than a substitute for legal safeguards and human oversight.

Legal Framework and Practical Implementation of Digital Social Supervision in Vietnam

Legal framework for citizen participation, digital governance and data

Citizen participation in anti-corruption constitutes an important component of Vietnam's broader framework for controlling the exercise of public power, rooted in the constitutional principle of building a "State of the people, by the people, and for the people", under which the people exercise their rights to participate in state governance and supervise the exercise of public power. Within this framework, social supervision enables citizens and social organizations to monitor the exercise of public authority,

detect violations, and communicate concerns to competent state bodies. Over time, the Communist Party of Vietnam (CPV) has consistently emphasized that anti-corruption is not solely the responsibility of state inspection and law-enforcement institutions, but a task requiring the participation of the entire political system and society. In this context, organizations such as the Vietnam Fatherland Front and grassroots supervisory bodies play an important role in facilitating public participation in overseeing state administration.

The legal framework has progressively translated this policy orientation into concrete rights and mechanisms for citizens. The Law on Anti-Corruption 2018, together with its subsequent amendments and implementing provisions, establishes a legal basis for citizens to report corrupt conduct and participate in the social monitoring of anti-corruption activities. The framework also recognizes the importance of protecting individuals who provide information and promotes public participation through protection mechanisms, rewards, and recommendations to improve institutional arrangements. These provisions are particularly significant in the digital context, as the effectiveness of citizen oversight increasingly depends not only on citizens' legal entitlement to report misconduct but also on their ability to submit, preserve, and transmit information through secure, legally recognized digital channels.

The digitalization of public governance has consequently established a new legal framework for the exercise of these rights. The Criminal Procedure Code 2015 (specifically under Point c, Clause 1 of Article 87, Article 99, and Article 107) recognizes electronic data as an independent category of evidence, thereby providing a legal basis for the collection, assessment, and use of digital information in judicial proceedings. This development is complemented by the Law on Electronic Transactions 2023 (specifically under Articles 7, 9, 10, 11, and Chapter III), which strengthens the legal recognition of electronic records, electronic transactions, and digital authentication in state management and social activities. The relevance of these provisions extends beyond routine electronic administration: they also establish the institutional conditions under which information submitted by citizens in digital form may be treated as legally meaningful, rather than as merely informal communication.

Broader national policies on digital transformation and data governance have reinforced this legal evolution. Resolution No. 57-NQ/TW^[1] and Resolution No. 66-NQ/TW^[2] of the CPV Politburo reflect a strategic orientation toward integrating science, technology, digital transformation, and data-driven governance into state functioning. At the legislative level, the 2024 Law on Data establishes a broader framework for managing, using, sharing, and protecting data, thereby recognizing data as a strategic resource for national governance. Decree No. 61/2026/ND-CP further develops mechanisms for collecting and using electronic data provided by organizations and individuals to detect and handle violations. Taken together, these instruments demonstrate a gradual shift from a predominantly paper-based and institutionally fragmented model toward a governance structure in which digital information can be collected, exchanged, and analyzed across administrative processes.

The significance of this transformation lies not simply in replacing paper records with electronic records, but in the potential to integrate citizen participation into a broader data-based governance architecture. When electronic transactions, digital identity, public-sector databases, and legally recognized electronic evidence operate within a coherent legal framework, citizen reports can move beyond isolated complaints and become inputs into institutional verification and risk detection. Nevertheless, the existence of these legal foundations does not by itself guarantee effective digital social supervision. Their practical value ultimately depends on how accessible digital platforms are to citizens, how securely information can be processed and cross-referenced, and whether legal safeguards can protect those who participate in supervision. The legal framework therefore provides an essential foundation, but its effectiveness must be assessed against how digital supervision mechanisms actually operate in practice.

VNeID and existing digital supervision mechanisms

Vietnam's digital government has increasingly created direct channels for citizens to communicate with public authorities. Among these platforms, Vietnam Electronic Identification (VNeID) has emerged as an important component of the national digital infrastructure developed by the Ministry of Public Security (MPS). By integrating verified digital identity with a range of public services and administrative functions, VNeID has the potential to reduce procedural intermediaries and facilitate more direct interaction between citizens and competent authorities. For social supervision, digital reporting functions give citizens a way to transmit information about security, public administration, or potential misconduct through an authenticated electronic environment. This represents a significant departure from conventional reporting mechanisms that often depend on physical submission, face-to-face communication, or multiple administrative intermediaries.

The practical value of such a platform lies in its ability to combine identity verification, digital transmission, and the submission of supporting materials within a single environment. Citizens may provide information in different digital forms, including photographs, audio or video recordings, and other electronic records relevant to the reported conduct. From a governance perspective, this facilitates the preservation and transmission of information while reducing some of the procedural burdens traditionally associated with citizen reporting. More importantly, digital submission creates the possibility of tracing the processing of information and integrating citizen-generated data into broader administrative systems. In principle, therefore, digital platforms can transform social supervision from an isolated act of reporting into a more continuous process involving submission, verification, processing, and institutional response.

However, the effectiveness of this model remains constrained by a number of institutional and technological bottlenecks. The first concerns the fragmentation of public-sector data. Administrative information in Vietnam remains distributed across different ministries, agencies, and levels of government, with varying technical standards and conditions for access and sharing. Where databases are not adequately interoperable, information submitted by citizens cannot easily be cross-referenced with other relevant

administrative records. This weakens the capacity of public authorities to verify information efficiently and may require the repeated collection of data that is already available elsewhere within the state apparatus. Consequently, although digital platforms may improve the transmission of information, they cannot by themselves overcome institutional fragmentation.

A second limitation concerns the relationship between citizen-generated information and the verification of public officials' assets and income. The development of the national system for controlling assets and income represents an important institutional foundation for detecting unexplained wealth and potential conflicts of interest. Nevertheless, the effectiveness of such a mechanism depends significantly on the ability to connect relevant information across administrative domains, including asset declarations, land records, and other legally accessible sources of financial and property information. Where such connections remain limited, verification continues to depend substantially on manual procedures and conventional inspection processes. Digital reporting therefore risks remaining reactive unless it can systematically incorporate citizen-generated information into broader verification and risk-assessment mechanisms.

A third bottleneck relates to the limited availability of public Open Data. Effective social supervision requires not only a channel for citizens to submit information, but also sufficient transparency that lets them identify irregularities independently. In areas such as public procurement, land-use planning, public investment, and budget execution, access to machine-readable and regularly updated datasets is particularly important for enabling citizens, civil society organizations, and journalists to compare information, identify anomalies, and generate evidence-based concerns. Where relevant data remain inaccessible, fragmented, or available only in non-machine-readable formats, society's capacity to perform independent oversight remains constrained. Digitalization of administrative procedures, therefore, should not be equated with transparency unless it is accompanied by meaningful and usable access to public information.

The fourth and perhaps most sensitive issue concerns the protection of persons who provide information. Digital platforms based on verified identity can increase accountability and reduce fraudulent reporting, but they may also generate concerns about exposure and retaliation. When citizens believe their identity can easily be linked to reports involving powerful officials or sensitive matters, a digital reporting channel may not be enough to encourage meaningful participation. This creates tension between two legitimate objectives: maintaining reliable user identification on the one hand and protecting legitimate whistleblowers from unauthorized disclosure on the other. The challenge, therefore, is not to eliminate identity verification, but to establish legal and technical mechanisms that let authorities verify the authenticity of information while limiting unnecessary access to the reporter's personal identity.

These limitations demonstrate that the principal challenge for Vietnam is no longer simply the digitization of citizen reporting. Rather, it lies in transforming separate digital functions into an integrated system of social supervision in which information can be securely submitted, independently verified, meaningfully cross-referenced, and effectively

acted upon. VNeID and other digital platforms provide an important institutional entry point, but their contribution to anti-corruption will remain limited unless accompanied by interoperable public databases, greater access to public information, stronger safeguards for whistleblowers, and clear procedures governing the use of citizen-generated electronic information. The current stage of digital governance may therefore be characterized as a transition from digitizing the channel of participation toward institutionalizing a comprehensive digital ecosystem for social supervision.

Legal and institutional limitations

Despite its potential to strengthen proactive anti-corruption governance, Big Data's application remains constrained by significant legal and institutional challenges. The first concerns the tension between extensive data processing and the protection of personal information. Big Data systems often require aggregating and reusing data originally collected for different administrative or commercial purposes, challenging traditional principles of purpose limitation, notice and consent, and data minimization (Zódi, 2017; Filatova-Bilous, 2022). In Vietnam, this tension is particularly evident when anti-corruption authorities seek to access sensitive financial, property, or transactional information, requiring a careful balance between legitimate investigative needs and privacy and data-protection rights (Phạm Hương Trà & Lê Nguyễn Ngọc Thảo, 2025).

A second limitation arises from the increasing reliance on algorithmic analysis. Big Data systems can identify unusual patterns and potential corruption risks, but algorithmic outputs do not necessarily establish that unlawful conduct has occurred. The risks of false positives, biased data, and opaque decision-making therefore require the continued involvement of human decision-makers. As emphasized in the literature on digital governance, the human-in-the-loop principle should ensure that algorithmic results remain analytical inputs subject to independent human verification rather than becoming automatic grounds for investigation or legal determination (Zódi, 2017; MindTitan, 2021; Chystiakova et al., 2025).

A third challenge concerns the legal status of digital information generated or identified through Big Data systems. Digital logs, metadata, transaction records, and algorithmic alerts may provide important investigative leads, but they do not automatically constitute admissible evidence. Their legal value depends on whether they have been lawfully collected, authenticated, preserved, and presented in accordance with procedural requirements. Vietnamese scholarship has accordingly emphasized the importance of technical verification and chain-of-custody mechanisms in ensuring the integrity of electronic evidence (Phạm Thúy Nga, 2023; Nguyễn Đức Hạnh, 2019; Wang, 2021).

Finally, the effectiveness of Big Data is limited by institutional fragmentation and data silos. Information relevant to corruption risks is often distributed across separate systems for taxation, land, banking, procurement, corporate registration, and personnel management, while legal and technical mechanisms for inter-agency data sharing remain insufficient. This fragmentation reduces the ability of authorities to combine relevant datasets and detect complex patterns of misconduct (Yu Wenxuan, 2025; Nguyễn Huy Hoàng & Vũ Đức Hoàn, 2024). Therefore, the

central challenge is not merely expanding data collection, but establishing a legal and institutional framework that enables lawful data sharing, secure integration, objective interpretation, and conversion into accountable anti-corruption action.

Comparative Experiences from Estonia and China

Estonia: Open Data, interoperability and data traceability

Estonia's approach to digital governance demonstrates that technology can support anti-corruption not merely by increasing administrative efficiency, but by strengthening transparency, interoperability, and citizens' ability to monitor the exercise of public authority. Since the early stages of digitalization, Estonia has developed a governance model in which separate public-sector information systems remain institutionally decentralized while being connected through common legal and technical standards. This approach is closely associated with principles such as openness, the once-only principle, and traceability, which together create the institutional conditions for data-driven public oversight (Kasemets & Lepp, 2010).

A key legal foundation is Estonia's Public Information Act, adopted in 2000. The Act establishes a general framework for public access to information held by public authorities and provides for the publication and re-use of open data. Where technically and proportionately feasible, public authorities are required to make open data available in machine-readable and open formats, while access remains subject to legitimate restrictions concerning privacy, national security, and other protected interests. This legal design is significant for anti-corruption because it enables citizens, researchers, journalists, and civil society organizations to independently examine public-sector information rather than relying exclusively on information supplied by administrative authorities.

The institutional effectiveness of this framework is reinforced by X-Road, Estonia's secure data-exchange infrastructure. Rather than establishing a single centralized database, X-Road enables independently managed information systems to exchange data securely across institutional boundaries. In conjunction with the once-only principle, citizens are generally not required to provide information repeatedly when the state already possesses it. This approach reduces unnecessary administrative interactions while enabling authorized agencies to access reliable information from other systems. Accordingly, the architecture shifts the emphasis from repeatedly collecting information to the secure and interoperable use of existing data, which is particularly relevant to identifying and verifying corruption-related risks.

Estonia also provides a distinctive mechanism for data traceability through the Data Tracker (Andmejälgija). Available through the national portal "eesti.ee", the system enables citizens to obtain an overview of operations performed with their personal data and thereby monitor how public authorities process their information. Because the system integrates with X-Road services, it can present access records in a standardized way across participating databases. This creates a form of "reverse supervision": instead of citizens merely being subject to administrative data processing, they are given visibility into how public institutions use their data.

Finally, Estonia complements interoperability and traceability with technological mechanisms for maintaining data integrity. The KSI Blockchain serves as an integrity-verification layer for selected government information systems, allowing authorities to detect unauthorized alterations to electronic records through cryptographic verification. At the same time, Estonia has explored artificial intelligence and machine-learning applications in areas such as tax-fraud detection, illustrating how interoperable data can support risk-based administrative supervision. These developments suggest that the principal lesson for Vietnam is not to replicate a particular technology, but to establish a coherent legal and institutional architecture in which open data enables public scrutiny, interoperability enables cross-institutional verification, and traceability enables accountability for data use.

China: Digital reporting, grassroots supervision and whistleblower protection

China's experience demonstrates how digital technologies can be integrated into a broader system of public participation in anti-corruption. According to R. Jianming and W. Fangfang (2019), public participation has evolved from a period of limited opportunities and willingness toward a more active model since the 18th National Congress of the Communist Party of China in 2012. Digital communication channels, including online reporting platforms and social media, have further expanded citizens' capacity to expose suspected corruption and provide information to supervisory authorities. Research by Pham Thi Duyen Thao and Pham Luong Khien (2025), together with Zhizhou et al. (2016), indicates that public reports and media disclosures have constituted an important source of corruption-related leads in China.

The expansion of digital reporting has been supported by a legal framework that increasingly recognizes the evidentiary value of electronic information and strengthens institutional mechanisms for supervision. As analyzed by Ran Wang (2021), amendments to China's Criminal Procedure Law formally recognized electronic data as an independent category of admissible evidence, while subsequent judicial and procedural rules established requirements for the extraction, preservation, and verification of such data. The 2018 Supervision Law further strengthened institutional integration by establishing the National Supervisory Commission and expanding the authority to collect and examine information relating to public officials. In parallel, regulations concerning whistleblower protection provide mechanisms for confidentiality and anonymous reporting, thereby seeking to reduce the risks associated with citizen participation in anti-corruption activities.

At the technological level, China has developed a multi-layered digital supervision architecture. Central reporting platforms operated by the CCDI and NSC enable citizens to submit complaints and supporting electronic materials, while grassroots "One-Click" platforms integrated into WeChat facilitate public monitoring of village-level budgets, procurement, subsidies, and land compensation. These reporting channels can be connected with broader Big Data systems that cross-reference information from different administrative databases, thereby enabling authorities to identify relationships and anomalies that may not be visible within a single database. The materials provided describe this architecture as extending across banking, property,

taxation, vehicle, and corporate information systems, illustrating a shift from isolated reporting toward integrated data-assisted supervision.

The Chinese model nevertheless reveals that technological capacity must be accompanied by effective institutional safeguards. The extensive integration of personal and administrative data may create risks of excessive surveillance and privacy intrusion, while dependence on centralized digital systems may generate new forms of “high-tech corruption” if system administrators are able to manipulate data, algorithms, or risk indicators without adequate independent oversight. The materials also identify the risk of over-reliance on central inspection mechanisms at the expense of permanent grassroots supervision. These

concerns suggest that the value of China’s experience for Vietnam lies not in replicating its centralized architecture, but in selectively adopting its mechanisms for digital reporting, electronic evidence, and data-supported supervision while maintaining clear limits on data access, independent oversight, and protection of individual rights.

Comparative assessment and lessons for Vietnam

The two models differ significantly in institutional design, but both demonstrate that effective digital social supervision requires more than simply establishing an online reporting channel. Their principal differences and points of relevance to Vietnam can be summarized through the following criteria:

Criteria	Estonia	China	Implications for Vietnam
Governance approach	Transparency, Open Data, interoperability	Centralized supervision and integrated data analysis	Combine transparency with coordinated data governance
Institutional architecture	Decentralized systems connected through X-Road	Centralized supervisory institutions and multi-level platforms	Develop interoperability without unnecessary institutional centralization
Technical infrastructure	X-Road, Data Tracker, data-integrity mechanisms	Digital reporting platforms, integrated Big Data systems, grassroots platforms	Connect VNeID and sectoral databases through secure interoperability
Citizen participation	Access to public information and monitoring of data use	Anonymous reporting, digital complaints, grassroots monitoring	Strengthen both reporting mechanisms and citizens’ access to public data
Electronic evidence	Emphasis on data integrity and traceability	Formal recognition and procedural regulation of electronic evidence	Further clarify authentication and chain-of-custody requirements
Whistleblower protection	Traceability of institutional data access	Confidential and anonymous reporting mechanisms	Strengthen identity protection and anti-retaliation safeguards
Principal risks	Digital exclusion and dependence on technical capacity	Privacy risks, centralized control, insider manipulation	Balance technological efficiency with rights protection and independent oversight

The comparison suggests that Vietnam does not need to reproduce either model in its entirety. Rather, Estonia offers a stronger reference point for Open Data, interoperability, and traceability, while China provides relevant experience in digital reporting, electronic evidence, and large-scale data-supported supervision. The central lesson is therefore to develop a hybrid legal and institutional framework that connects digital citizen reporting to interoperable public databases, meaningful access to public information, reliable electronic evidence, and effective safeguards for personal data and whistleblowers.

Recommendations for Strengthening Digital Social Supervision in Vietnam

The comparative analysis indicates that strengthening digital social supervision in Vietnam requires more than expanding digital reporting platforms. Its effectiveness depends on simultaneously developing legal safeguards, interoperable data infrastructure, public access to information, and institutional mechanisms to control technology use. Accordingly, reform should focus on three interconnected priorities: protecting citizens who provide information, improving data interoperability and openness, and ensuring meaningful human oversight over data-driven decision-making.

1. Strengthening Digital Identity Protection and Whistleblower Safeguards

The first priority is to create a secure legal and technological environment in which citizens can report suspected corruption without facing disproportionate risks of identity exposure or retaliation. Vietnam should therefore develop

mechanisms for pseudonymization and encryption of digital reports submitted through VNeID, while maintaining the ability of competent authorities to verify the reporter’s identity when legally necessary. The legal framework should clearly regulate who may access identity information, under what circumstances disclosure may occur, and what remedies are available in cases of unauthorized disclosure. In parallel, Vietnam may consider strengthening incentives for verified information that contributes materially to the recovery of illicit assets, together with stricter sanctions for violations of whistleblower confidentiality.

2. Expanding Open Data and Interoperable Anti-Corruption Data Infrastructure

The second priority is to move from fragmented administrative databases toward a more interoperable data environment. Relevant information from VNeID and the asset and income control system should, subject to legal authorization and data-protection requirements, be capable of being cross-referenced with land, taxation, procurement, and other relevant public databases. Such interoperability would allow authorities to identify inconsistencies and potential risks more efficiently while reducing dependence on repeated manual verification. At the same time, Vietnam should expand machine-readable Open Data in high-risk sectors such as public procurement, land-use planning, public investment, and budget execution. Greater public access to structured information would enable citizens, the Vietnam Fatherland Front, supervisory bodies, journalists, and civil society to undertake more substantive and evidence-based social supervision.

3. Maintaining Human Oversight and Technical Accountability

The third priority is to ensure that technological systems remain instruments of decision support rather than autonomous substitutes for legal judgment. Big Data analytics and algorithmic risk scores should therefore be treated as investigative signals requiring independent human verification before any administrative, disciplinary, or judicial action is taken. This human-in-the-loop approach should be accompanied by technical accountability mechanisms, including comprehensive access logs, dual authorization for sensitive data, and periodic independent audits of data systems and algorithms. Such safeguards are particularly important because the digitalization of anti-corruption governance may itself generate new forms of abuse, including unauthorized data manipulation or suppression of risk indicators.

Taken together, these reforms would enable Vietnam to move from merely digitizing citizen reporting toward establishing a broader digital social supervision framework. The objective should not be to maximize data collection or automate anti-corruption decisions, but to create a system in which citizens can safely participate, public information is meaningfully accessible, relevant databases can be lawfully interconnected, and technological outputs remain subject to transparent and accountable human oversight.

Conclusion

Applying Big Data to anti-corruption marks an important shift in public power oversight, moving from predominantly reactive inspection to proactive, data-driven risk identification and prevention. By enabling the integration, cross-referencing, and analysis of large volumes of information from multiple sources, Big Data can strengthen public authorities' and citizens' capacity to identify irregularities and potential corruption risks earlier. However, technological capacity alone cannot ensure effective anti-corruption governance; its effectiveness depends on an appropriate legal and institutional framework.

The comparative analysis of Estonia and China demonstrates two distinct approaches to technology-enabled integrity governance. Estonia emphasizes Open Data, interoperability, and traceability, while China places greater emphasis on digital reporting, centralized data integration, and institutionalized supervisory mechanisms. Despite their different institutional structures, both experiences show the importance of integrating digital infrastructure with legal safeguards, reliable data governance, and mechanisms that enable citizens to monitor the exercise of public power.

For Vietnam, the principal challenges remain fragmented administrative databases, limitations in the use and verification of electronic information, restricted access to relevant public data, and concerns regarding the protection of citizens who provide information. Addressing these barriers requires a coherent digital supervision framework that strengthens interoperability among relevant public databases, expands access to machine-readable Open Data, improves the procedural framework for electronic evidence, and provides effective protection for whistleblowers using digital reporting channels.

Ultimately, digital transformation should strengthen accountable and rights-protective governance rather than replace legal and institutional safeguards. Big Data and

algorithmic systems should therefore remain subject to human oversight, procedural guarantees, and mechanisms of institutional accountability. A balanced combination of technological capacity, legal certainty, data transparency, and citizen protection would provide a more sustainable foundation for strengthening social supervision and preventing corruption in Vietnam's digital governance environment.

References

1. Resolution No. 57-NQ/TW dated 22 December 2024 issued by the Politburo of the CPV on Breakthrough Development in Science and Technology, Innovation and National Digital Transformation.
2. Resolution No. 66-NQ/TW dated 30 April 2025 issued by the Politburo of the CPV on Reforming Law-Making and Law Enforcement to Meet the Requirements of National Development in the New Era.
3. Al-Ababneh HA, Fedorchuk Y, Tymchyshyn A, Pishchenko G, Hrytsai S. The use of big data in the detection of economic crimes in public procurements. *Journal of Theoretical and Applied Information Technology*,2024;102(24):8860-8871.
4. Aixin L. On the public participation in the construction of a clean government culture in my country. *Research on a Clean Government Culture*,2020;11(5):1-8.
5. Chystiakova A, Podliehaiev K, Khoronovskiy O, Sokur T, Kubariev I. The role of big data analytics in the investigation of corruption offences. *Revistas. Rcaap.Pt*,2025;37(1):1-12.
6. Dobrovolska O, Rozhkova M. The impact of digital transformation on the anti-corruption and cyber-fraud system. *Business Ethics and Leadership*,2024;8(3):232-241.
7. Filatova-Bilous N. Data as a tradeable commodity: Propertization vs. the concept of exclusive rights. *Teisė*,2022;124(1):36-48.
8. Government of Vietnam. Decree No. 61/2026/ND-CP dated 13 February 2026 on the List, Management and Use of Professional Technical Means and Equipment, and Procedures for Collecting and Using Data Obtained from Technical Means and Equipment Provided by Individuals and Organizations to Detect Administrative Violations.
9. Government of Vietnam. Resolution No. 168/NQ-CP dated 11 October 2023 promulgating the National Strategy on Anti-Corruption and Negative Phenomena Prevention and Control to 2030.
10. Jianming R, Fangfang W. Modes and changes of public participation in anti-corruption in the 40 years of reform and opening up. *Journal of Beihang University (Social Science Edition)*,2019;32(1):1-10.
11. Kasemets A, Lepp Ü. Anti-corruption programmes, studies and projects in Estonia 1997–2009. *Civil Society as Anti-Corruption Actor*,2010;1(1):40-55.
12. Kovačević D. Transforming governance: Harnessing new technologies in the fight against corruption. *Institute for Sociological, Political and Juridical Research Conference Proceedings*,2024;12(1):95-112.
13. MindTitan. AI use cases for government: How Estonia is leading the way. *Government Technology and AI Review*,2021;4(2):1-15.

14. National Assembly of Vietnam. Constitution of the Socialist Republic of Vietnam (2013), as amended by Resolution No. 203/2025/QH15 dated 16 June 2025; Consolidated Version No. 52/VBHN-VPQH dated 21 July 2025.
15. National Assembly of Vietnam. Criminal Procedure Code No. 101/2015/QH13, as amended, including by Law No. 99/2025/QH15; Articles 87(1) and 99 on electronic data and evidence.
16. National Assembly of Vietnam. Law on Anti-Corruption No. 36/2018/QH14.
17. National Assembly of Vietnam. Law on Data No. 60/2024/QH15.
18. National Assembly of Vietnam. Law on Electronic Transactions No. 20/2023/QH15.
19. National People's Congress of the People's Republic of China. Criminal Procedure Law of the People's Republic of China (amended in 2012 and 2018), Article 50 on electronic data evidence.
20. National People's Congress of the People's Republic of China. Supervision Law of the People's Republic of China (adopted 20 March 2018).
21. Nguyễn ĐH. Dữ liệu điện tử và chứng cứ điện tử. Tạp chí Khoa học Kiểm sát, 2019;15(1):37-42.
22. Nguyễn HH, Đào TH. Ứng dụng công nghệ số trong hoạt động thanh tra, tiếp công dân, giải quyết khiếu nại, tố cáo và phòng, chống tham nhũng. Tạp chí Quản lý nhà nước, 2025;35(354):54-58.
23. Nguyễn HH, Vũ ĐH. Tăng cường ứng dụng công nghệ số trong thanh tra, tiếp công dân, giải quyết khiếu nại, tố cáo và phòng, chống tham nhũng. Tạp chí Thanh tra, 2024;24(10):62-66.
24. Odilla F, Mattoni A. Unveiling the layers of data activism: The organising of civic innovation to fight corruption in Brazil. *Big Data & Society*, 2023;10(2):1-15.
25. Parliament of Estonia. Public Information Act (passed 15 November 2000, RT I 2000, 92, 597).
26. Parliament of Estonia. Public Procurement Act (passed 14 June 2017, RT I, 01.07.2017, 1).
27. Phạm HT, Lê NNT. Ứng dụng trí tuệ nhân tạo và dữ liệu lớn trong phòng, chống tham nhũng và gian lận tài chính tại Việt Nam. Tạp chí Cộng sản, 2025;103(1091):1-8.
28. Phạm TN. Ứng dụng trí tuệ nhân tạo và phân tích dữ liệu lớn trong điều tra tội phạm – Kinh nghiệm của các quốc gia trên thế giới và một số gợi ý cho Việt Nam. Tạp chí Dân chủ và Pháp luật, 2023;67(5):42-48.
29. Phạm TDT, Phạm LK. Sự tham gia của Nhân dân trong phòng chống tham nhũng ở Trung Quốc và một số kinh nghiệm cho Việt Nam. Tạp chí Nghề Luật, 2025;20(2):83-90.
30. Politburo of the Communist Party of Vietnam. Resolution No. 57-NQ/TW dated 22 December 2024 on Breakthroughs in the Development of Science and Technology, Innovation, and National Digital Transformation.
31. Politburo of the Communist Party of Vietnam. Resolution No. 66-NQ/TW dated 30 April 2025 on Reforming Lawmaking and Law Enforcement to Meet the Requirements of National Development in the New Era.
32. Rosnidah I, Johari RJ, Hairudin NAM, Hussin SASH, Musyaffi AM. Detecting and preventing fraud with big data analytics: Auditing perspective. *Journal of Governance and Regulation*, 2022;11(4):8-15.
33. Wang R. Experience of big data anti-corruption in China. *Research Handbook on Big Data Law*, 2021;1(1):150-170.
34. Yu W. Technologies facilitate anti-corruption governance. *China Daily*, 2025;45(106):1-4.
35. Zhizhou D, Yanfei L, Wenguan G. The history and characteristics of people's participation in anti-corruption since the founding of the People's Republic of China. *Journal of Guangzhou University (Social Science Edition)*, 2016;15(1):1-12.
36. Zöldi Z. Law and legal science in the age of big data. *Intersections. East European Journal of Society and Politics*, 2017;3(2):69-87.