

Applying Digital Technology to Protect Whistleblowers Reporting Corruption in Vietnam

Vu Van Chi^{1*}

^{1*} *University of Law, Vietnam National University, Hanoi;*
Corresponding Author: Vu Van Chi

Abstract:

Whistleblower protection is a critical component of effective anti-corruption governance, as individuals who report corruption often face significant risks of retaliation, discrimination, reputational harm, and threats to their employment, property, or personal safety. In the context of rapid digital transformation, digital technologies offer new opportunities to strengthen the confidentiality, security, accessibility, and accountability of whistleblowing mechanisms. This article examines the potential role of digital technology in enhancing the protection of whistleblowers reporting corruption in Vietnam. It first reviews the existing legal and policy framework governing whistleblower protection, with particular attention to the Law on Denunciations 2018, the Law on Anti-Corruption 2018, and relevant implementing regulations. It then examines international approaches, particularly the European Union, South Korea, and Singapore, to identify technological and institutional practices that may be relevant to Vietnam. The study employs doctrinal legal analysis, comparative legal analysis, and policy analysis, complemented by selected empirical evidence from the PAPI surveys, UNDP reports, and Transparency International. The findings indicate that, although Vietnam has established a relatively comprehensive legal framework for protecting whistleblowers, the existing system has not yet fully incorporated the requirements of the digital environment. In particular, gaps remain in relation to secure electronic reporting, digital anonymity, data protection, cybersecurity, independent oversight, and the governance of digital evidence. The article argues that digitalization should not be understood merely as the electronic conversion of existing reporting procedures, but as an institutional transformation integrating legal safeguards with encryption, secure digital reporting platforms, artificial intelligence-assisted processing, and tamper-resistant data management. On this basis, the article proposes policy directions for developing a secure and accountable digital whistleblower protection mechanism in Vietnam, while addressing the risks of misuse, data breaches, and conflicts between confidentiality and procedural fairness.

Keywords: whistleblower protection; corruption reporting; digital technology; e-whistleblowing; anti-corruption; data protection; Vietnam.

1. Introduction

Whistleblowing is widely recognized as an important mechanism for detecting and exposing corruption, particularly where misconduct occurs within public institutions or organizational environments that are difficult to monitor through conventional oversight mechanisms. By providing information that may otherwise remain inaccessible to law enforcement and inspection bodies, whistleblowers contribute to transparency, accountability, and public participation in anti-corruption governance. Effective protection is therefore not only a matter of safeguarding individual rights but also an institutional condition for encouraging reporting and strengthening organizational integrity (OECD, 2016).

Vietnam has progressively developed a legal framework for whistleblower protection. The 2013 Constitution recognizes citizens' right to lodge complaints and denunciations, while the Law on

Denunciations 2018 and the Law on Anti-Corruption 2018 provide more specific safeguards concerning confidentiality and the protection of whistleblowers' life, health, honor, dignity, employment, income, and property. Decree No. 31/2019/ND-CP further specifies procedures and responsibilities for implementing protective measures. Nevertheless, these mechanisms remain largely designed around conventional administrative and legal procedures. Existing electronic reporting channels have often focused on digitizing submission rather than establishing secure, technologically integrated systems capable of addressing risks such as identity disclosure, cyberattacks, and retaliation.

This limitation is increasingly important as Vietnam advances digital transformation and data-driven public governance. National policies emphasize the use of digital technologies in public administration, institutional reform, and anti-corruption efforts, creating an opportunity to

reconsider whistleblower protection from a digital governance perspective. Technologies such as secure online reporting platforms, encryption, digital identity management, artificial intelligence (AI), blockchain-based data integrity mechanisms, and data analytics may strengthen confidentiality, facilitate reporting, improve case management, and enhance institutional accountability. However, technological solutions must be embedded within appropriate legal and institutional safeguards.

International experience provides useful reference points. Directive (EU) 2019/1937 establishes standards for secure internal and external reporting channels and the protection of reporting persons. South Korea's Anti-Corruption and Civil Rights Commission (ACRC) has developed the Clean Portal, while Singapore's Corrupt Practices Investigation Bureau (CPIB) provides electronic reporting channels for corruption. These experiences demonstrate that effective digital whistleblowing requires the integration of technology, confidentiality, legal protection, and institutional responsiveness. Research on online whistleblowing systems similarly indicates that users' perceptions of security, trust, and the characteristics of reporting systems influence their willingness to use such mechanisms (Lowry et al., 2013).

Against this background, this article examines the potential of digital technology to strengthen the protection of whistleblowers reporting corruption in Vietnam. It addresses three questions: (1) whether the existing Vietnamese legal and policy framework provides an adequate basis for protection in the digital environment; (2) what technological and institutional practices from selected jurisdictions may provide useful lessons for Vietnam; and (3) what legal, technological, institutional, and social challenges must be addressed to establish an effective digital whistleblower protection mechanism.

The article contributes to the existing discussion in two respects. First, it connects the legal-institutional issue of whistleblower protection with digital governance and cybersecurity. Second, it conceptualizes digital whistleblower protection not merely as the electronic submission of reports but as an integrated mechanism combining confidentiality, data security, technological infrastructure, institutional accountability, and legal safeguards. On this basis, the article proposes policy

directions for strengthening whistleblower protection in Vietnam while addressing digital risks, including identity disclosure, data breaches, abusive reporting, and the need to balance confidentiality with procedural fairness.

2. Methodology

This study adopts a qualitative and interdisciplinary research design combining doctrinal legal analysis, comparative legal and policy analysis, and contextual analysis. The methodology examines not only Vietnam's formal legal framework for whistleblower protection but also the institutional, technological, and social conditions required for its effective implementation in a digital governance environment.

First, doctrinal legal analysis is used to examine the principal Vietnamese legal and policy instruments governing whistleblowing and whistleblower protection, including the Constitution, the Law on Denunciations 2018, the Law on Anti-Corruption 2018, Decree No. 31/2019/ND-CP, and relevant regulations on digital governance, cybersecurity, and personal data protection. Particular attention is given to confidentiality, protection against retaliation, protection of personal interests, institutional responsibilities, and procedures for applying protective measures. This analysis identifies both the strengths of the existing framework and regulatory gaps arising from digital reporting.

Second, comparative legal and policy analysis examines selected experiences from the European Union, South Korea, and Singapore, which have developed institutional and digital mechanisms for receiving and managing reports of misconduct. The comparison focuses on secure reporting channels, confidentiality and anonymity, data security, technological applications, institutional responsibilities, and protection against retaliation. The purpose is not to transplant foreign models directly but to identify principles and practices that may be adapted to Vietnam's legal and administrative context.

Third, the study uses policy analysis and selected empirical evidence from sources including the Vietnam Provincial Governance and Public Administration Performance Index (PAPI), UNDP reports, and Transparency International to contextualize public perceptions of corruption, governance, and accountability. These sources are used as contextual evidence rather than for causal

inference. The study does not conduct an original quantitative survey or statistical analysis.

Finally, a problem-oriented analytical framework is applied across four dimensions: (1) legal and institutional adequacy; (2) technological capacity, including secure digital reporting, encryption, AI-assisted processing, and tamper-resistant data management; (3) social and organizational conditions affecting trust and willingness to report; and (4) risks related to cybersecurity, data leakage, misuse of anonymous reporting, and the balance between confidentiality and procedural fairness.

By combining these approaches, the study moves beyond a descriptive assessment of Vietnamese law to examine how legal protection and digital technologies can be integrated into a coherent mechanism for protecting whistleblowers reporting corruption. The findings provide the analytical basis for the policy recommendations presented in the final section.

3. Results and Discussion

3.1. The Imperative of Protecting Whistleblowers Reporting Corruption in the Context of Digital Governance in Vietnam

Whistleblowing generally refers to the disclosure of information concerning wrongdoing to competent authorities or, in certain circumstances, to the public. In the Vietnamese legal context, denunciation (tố cáo) means informing a competent person, agency, or organization of an alleged violation of law for examination and appropriate action (Center for Vietnamese Lexicography, 2009). Accordingly, whistleblowing in relation to corruption may be understood as reporting suspected corrupt conduct to competent authorities for investigation and resolution. Although whistleblowing is only one component of the broader anti-corruption framework, it is particularly important because corruption is often concealed within institutional environments that conventional monitoring mechanisms cannot easily penetrate.

The importance of whistleblowing is widely recognized in international anti-corruption standards. The OECD emphasizes that effective whistleblower protection is essential for safeguarding the public interest, promoting integrity and accountability, and encouraging the reporting of misconduct, fraud, and corruption (OECD, 2016). Similarly, the United Nations Office on Drugs and Crime (UNODC) identifies the encouragement and

protection of reporting persons as an important element of an effective anti-corruption framework. Retaliation may affect not only whistleblowers but also their families and colleagues, thereby discouraging future reporting (UNODC, 2015).

Protection is particularly important in corruption cases because reported persons may possess official authority, organizational influence, or institutional resources, while whistleblowers may occupy a comparatively weaker position (Vu Cong Giao & Tran Thuy Duong, 2024). They may face retaliation, discrimination, reputational damage, loss of employment or income, threats to property, or even threats to physical safety. In the digital environment, these risks are amplified by the rapid disclosure and dissemination of personal information through online platforms. Consequently, effective anti-corruption reporting depends not only on citizens' willingness to report but also on the credibility, accessibility, confidentiality, and responsiveness of the protection mechanisms available to them (OECD, 2016; UNODC, 2015).

The United Nations Convention against Corruption (UNCAC) provides an important international legal basis for such protection. Article 32 calls for appropriate measures to protect witnesses and, where appropriate, their relatives and other persons close to them against retaliation or intimidation. Article 33 further calls for appropriate measures to protect persons who report, in good faith and on reasonable grounds, facts concerning offences established under the Convention (United Nations, 2004). As a State Party to UNCAC, Vietnam therefore has an important international commitment to strengthen domestic mechanisms for protecting persons who report corruption.

This commitment is reflected in Vietnam's domestic legal framework. The 2013 Constitution recognizes citizens' right to lodge complaints and denunciations, while the Law on Denunciations 2018 and the Law on Anti-Corruption 2018 provide safeguards concerning confidentiality and protection against retaliation. Decree No. 31/2019/ND-CP further specifies the implementation of protective measures. The framework therefore provides a relatively broad legal basis for protecting life, health, honor, dignity, employment, income, and property, as well as, where appropriate, the interests of relatives. However, formal legal protection does not necessarily ensure citizens' willingness to report

corruption. If potential whistleblowers believe that their identities may be disclosed, complaints may not be handled impartially, or retaliation cannot be effectively prevented, formal rights may have limited practical value (OECD, 2016; UNODC, 2015).

This issue has become increasingly significant as Vietnam promotes digital transformation and digital governance. Digitalization of whistleblower protection should not simply replace paper-based reporting with electronic submission; rather, it should redesign reporting and protection processes around confidentiality, data security, accessibility, traceability, and institutional accountability (Melley, 2020). Evidence from the 2023 Provincial Governance and Public Administration Performance Index (PAPI), based on responses from 19,536 citizens, provides important evidence on perceptions and experiences concerning governance, corruption control, transparency, accountability, and e-government in Vietnam (United Nations Development Programme [UNDP], 2024a, 2024b). Meanwhile, Transparency International's 2023 Corruption Perceptions Index gave Vietnam a score of 41/100 and ranked it 83rd among 180 countries and territories. Although the CPI does not directly measure whistleblower protection, it provides relevant contextual evidence of the continuing need to strengthen anti-corruption institutions and public accountability (Transparency International, 2024).

Whistleblowing also has an important detection function. The OECD identifies whistleblowers and whistleblower protection as significant sources and mechanisms for detecting foreign bribery and related offences (OECD, 2017). Inadequate protection may therefore weaken not only individual rights but also the State's ability to obtain information about otherwise concealed misconduct.

Digital technologies create both opportunities and risks. Secure online reporting platforms can reduce geographical and administrative barriers, facilitate communication with authorities, and improve the monitoring of case processing. Conversely, digitalization may create vulnerabilities such as unauthorized access, metadata exposure, cyberattacks, device compromise, and rapid dissemination of sensitive information. Its protective effect therefore depends

on system architecture, data governance, and institutional safeguards.

Research supports the importance of trust and anonymity in online whistleblowing. Lowry et al. (2013) found that anonymity, trust, and perceived risk are particularly important in online reporting systems. However, digital anonymity is more complex than simply removing a person's name because digital systems may generate information capable of identifying or profiling users. Berendt and Schiffner (2021) similarly argue that technological anonymity alone is insufficient and must be combined with legal protection and appropriate organizational practices. Digital whistleblower protection should therefore be understood as a governance issue involving law, technology, institutional culture, and data protection.

Accordingly, an effective digital whistleblower protection mechanism should rest on three mutually reinforcing foundations. First, public trust and social acceptance: citizens must have reasonable confidence that digital reporting is confidential, secure, and legally protected. Second, institutional and technological capacity: competent authorities must be able to operate secure reporting systems, protect sensitive information, and manage reports throughout their lifecycle, with technologies such as encryption, secure authentication, privacy-enhancing techniques, and AI-assisted classification used under appropriate human oversight. Third, sustainable resources and governance arrangements: effective protection requires adequate funding, qualified personnel, cybersecurity capacity, interoperable infrastructure, and clearly defined institutional responsibilities.

From this perspective, Vietnam's principal challenge is not simply the introduction of artificial intelligence, blockchain, encryption, or electronic reporting platforms, but their integration into a coherent legal and institutional framework. The Law on Denunciations 2018 provides an important foundation, but the technological dimensions of confidentiality, digital anonymity, cybersecurity, and secure electronic reporting remain insufficiently developed. The key gap is therefore between a largely traditional protection framework and the technological realities of contemporary governance.

Digital whistleblower protection should also not be equated with anonymous reporting alone. Excessive reliance on anonymity may complicate

information verification, communication with whistleblowers, and procedural fairness for persons accused of wrongdoing. A more sustainable model should combine confidential reporting, carefully designed anonymity options, secure communication, strong data protection, risk-based protection measures, and clear procedures for evaluating reports. Such an integrated approach can protect both whistleblowers and persons accused of wrongdoing while strengthening the State's capacity to detect and respond to corruption.

Ultimately, digital transformation should be understood as an institutional reform of whistleblower protection rather than merely a technological upgrade. Vietnam should therefore harmonize the Law on Denunciations with cybersecurity and personal data protection legislation, establish standards for secure electronic reporting, clarify institutional responsibility for data breaches and retaliation, and strengthen independent oversight. An integrated approach of this kind would enable digitalization to contribute substantively to stronger whistleblower protection and, ultimately, to more effective, transparent, and accountable anti-corruption governance in Vietnam.

3.2. Vietnam's Policy and Legal Framework for Protecting Whistleblowers Reporting Corruption in the Digital Era

The protection of whistleblowers reporting corruption has long been recognized in Vietnam's legal framework. The right to lodge complaints and denunciations was first recognized in the 1959 Constitution (Article 29) and subsequently reaffirmed in later constitutions. The 1980 Constitution expressly prohibited retaliation against persons making complaints or denunciations (Article 73), a principle maintained in the 1992 Constitution and reaffirmed in Article 30 of the 2013 Constitution.

Building on this constitutional foundation, Vietnam has progressively developed legal provisions on corruption reporting and whistleblower protection. Relevant provisions appeared in the Law on Anti-Corruption 2005, as amended in 2007 and 2012, and were further strengthened in the Law on Anti-Corruption 2018. Under Article 5 of the 2018 Law, reporting corruption is recognized as both a right and an obligation of citizens. Article 4 requires competent agencies, organizations, and units to receive and promptly process reports and protect the lawful rights and interests of persons who report or provide

information concerning corrupt conduct. Article 8 prohibits threats, retaliation, victimization, and disclosure of information concerning such persons, while Article 65 specifically provides for confidentiality regarding information about persons who discover, report, denounce, expose, notify, or otherwise provide information on corruption. Decree No. 120/2006/ND-CP and Decree No. 59/2013/ND-CP further provided guidance for implementing the anti-corruption legislation.

These developments demonstrate a gradual shift from a general constitutional prohibition of retaliation toward a more comprehensive statutory protection framework. The 2013 Constitution, the Law on Denunciations 2018, and the Law on Anti-Corruption 2018 establish protection concerning confidentiality, life, health, honor, dignity, property, employment, and income, with protection potentially extending to relatives. Decree No. 31/2019/ND-CP further specifies protective measures and the responsibilities of relevant authorities, while Circular No. 145/2020/TT-BCA provides for police responsibilities in protecting whistleblowers and their relatives where there are risks of threats or retaliation. This framework is broadly consistent with Article 33 of the United Nations Convention against Corruption (UNCAC), which calls for appropriate measures to protect persons reporting corruption-related offences against unjustified treatment (United Nations, 2004).

At the policy level, Vietnam has also established a broader orientation linking anti-corruption, rule-of-law development, and digital transformation. Resolution No. 27-NQ/TW of 2022 emphasizes the protection of human and citizens' rights in building the Socialist rule-of-law State. Resolution No. 52-NQ/TW of 2019 identifies the application of digital technologies in public administration, monitoring, and anti-corruption as an important strategic direction, while Resolution No. 57-NQ/TW of 2024 further emphasizes science, technology, innovation, and national digital transformation. Resolutions Nos. 60-NQ/TW and 66-NQ/TW of 2025 reinforce administrative restructuring and reform of law-making and law-enforcement processes. Together, these policies provide a clear basis for integrating digital technologies into mechanisms for transparency, accountability, and corruption reporting.

Nevertheless, the existing framework remains primarily oriented toward conventional

administrative and legal protection. Its regulation of digital-specific risks—including unauthorized disclosure of personal information, cyberattacks, metadata exposure, digital identification, and secure electronic reporting—remains insufficiently developed. In a digital environment, confidentiality cannot be guaranteed simply by prohibiting disclosure of a whistleblower's name because reporting systems may generate IP addresses, timestamps, device identifiers, access logs, and other metadata capable of revealing identity. Effective digital protection therefore requires both legal confidentiality and technical safeguards.

International experience provides useful guidance. The OECD emphasizes that effective whistleblower protection requires accessible reporting channels, confidentiality, protection against retaliation, and credible institutional responses (OECD, 2016). Similarly, Directive (EU) 2019/1937 requires secure internal and external reporting channels, confidentiality of reporting persons' identities, restricted access, appropriate follow-up, and protection of personal data. It also recognizes online platforms as potential reporting channels (European Parliament & Council of the European Union, 2019). Importantly, the European framework demonstrates that digital reporting should not be reduced to creating an electronic mailbox; it requires an integrated institutional architecture combining secure technology, confidentiality, impartial follow-up, and accountability.

Berendt and Schiffner (2021) further emphasize that technological anonymity alone cannot guarantee effective whistleblower protection. Technical safeguards must be combined with legal protection, organizational practices, and appropriate institutional norms. This is particularly relevant to Vietnam, where digitalization should be accompanied by reforms in data governance, institutional responsibility, and organizational culture.

In practice, Vietnamese ministries, agencies, and local authorities have increasingly accepted denunciations through online public services and official electronic channels. However, these mechanisms have largely focused on digitizing the submission process rather than developing comprehensive digital protection. Important issues such as anonymous or pseudonymous reporting, metadata protection, specialized cybersecurity safeguards, and secure communication remain

insufficiently addressed. Consequently, potential whistleblowers may still hesitate to use digital channels if they fear identity disclosure or retaliation. As the OECD notes, fear of retaliation and the absence of a credible institutional response can significantly discourage reporting (OECD, 2016).

The current framework can therefore be assessed from four perspectives. First, its major strength is the relatively broad legal protection of whistleblowers and their important personal and socio-economic interests. Second, it benefits from a consistent policy orientation linking anti-corruption, rule-of-law development, and digital transformation. Third, its major weakness is the limited integration of digital security requirements, particularly regarding metadata, technical anonymity, cybersecurity, data retention, and independent oversight. Fourth, Vietnam's expanding digital infrastructure, including national databases, electronic identification, digital signatures, and e-government platforms, provides an important opportunity to establish more secure reporting mechanisms.

At the same time, digitalization raises several challenges. The first concerns the balance between anonymity and accountability. Complete anonymity may encourage reporting by reducing retaliation risks, but it can also complicate verification and communication. Directive (EU) 2019/1937 therefore distinguishes confidentiality from anonymous reporting and leaves certain aspects of anonymous reporting to Member States (European Parliament & Council of the European Union, 2019). The second concerns data governance, as whistleblower reports may contain sensitive information about reporting persons, accused persons, witnesses, relatives, and colleagues. Effective systems therefore require clear rules on data collection, access control, encryption, retention, deletion, disclosure, and incident response. The third concerns institutional independence and accountability: secure technology cannot compensate for weak institutional safeguards, conflicts of interest, unauthorized access, or ineffective remedies for retaliation.

Accordingly, Vietnam has established an important legal foundation for whistleblower protection but has not yet developed a fully integrated digital protection architecture. The key challenge is therefore not simply the absence of legal rules, but the limited integration of

whistleblower protection with cybersecurity, personal data protection, and secure electronic reporting. Vietnam's digital infrastructure creates favorable conditions for addressing this gap through encrypted communication, controlled access, secure reporting, pseudonymous or anonymous reporting where appropriate, tamper-evident record management, and automated case tracking. Artificial intelligence may also assist in classifying and prioritizing reports, provided that its use remains subject to human oversight, transparency, data protection, and procedural safeguards.

Therefore, the immediate policy priority is to develop a digitally integrated whistleblower protection framework that connects the Law on Denunciations, the Law on Anti-Corruption, cybersecurity and personal-data regulations, and digital-government policies through common standards for confidentiality, secure reporting, data governance, accountability, and oversight. Rather than seeking "absolute" security, which no digital system can guarantee, Vietnam should establish a risk-based, multilayered protection architecture capable of minimizing identity disclosure, retaliation, data breaches, and other forms of digital harm. Such an integrated approach would enable digital transformation to contribute substantively to protecting whistleblowers and strengthening transparency, integrity, and accountability in Vietnam's digital governance.

3.3. Practical Potential of Digital Technologies for Protecting Whistleblowers Reporting Corruption

Against the backdrop of global digital transformation, digital technologies are increasingly being used to strengthen whistleblower protection, reflecting a shift from traditional administrative approaches toward governance models emphasizing transparency, security, accountability, and data-driven decision-making. Electronic whistleblowing systems and secure reporting channels can facilitate reporting, protect confidentiality, improve institutional monitoring, and reduce retaliation risks. Encryption and other privacy-enhancing technologies can further create safer communication environments between whistleblowers and receiving institutions (Di Salvo, 2020).

Within the European Union, Directive (EU) 2019/1937 provides a comprehensive framework for secure reporting channels. It requires relevant public and private entities to establish secure

internal reporting procedures, protect reporting persons' identities, prevent unauthorized access, and provide independent external reporting channels. Online platforms are recognized as potential reporting channels, but the Directive emphasizes confidentiality, restricted access, secure data processing, follow-up, and protection against retaliation rather than equating digital reporting with complete anonymity (European Parliament & Council of the European Union, 2019).

South Korea provides another relevant example through the Clean Portal operated by the Anti-Corruption and Civil Rights Commission (ACRC). The system enables online reporting of violations and corruption-related matters and provides measures including confidentiality, employment-related protection, and physical protection for whistleblowers and cooperating persons. Reports may be referred to relevant investigative or supervisory authorities, with reporting persons informed of the results (Anti-Corruption and Civil Rights Commission [ACRC], n.d.). Singapore has similarly developed the Corrupt Practices Investigation Bureau (CPIB)'s e-Report service, which allows online reporting of suspected corruption. Informants' identities are protected by law, and individuals may choose to remain anonymous (Corrupt Practices Investigation Bureau [CPIB], 2026).

These experiences demonstrate that digital whistleblower protection involves more than converting paper-based reporting into electronic forms. It requires secure reporting channels, confidentiality, controlled access, data governance, secure storage, and effective follow-up. As Berendt and Schiffner (2021) emphasize, technological anonymity alone is insufficient; effective protection requires the combination of technical safeguards, legal protection, and appropriate organizational practices.

For Vietnam, the practical potential of digital technologies can be considered from four major perspectives.

First, blockchain technology may strengthen the integrity and traceability of reporting records. A permissioned blockchain or distributed-ledger architecture could create tamper-evident records of submission, access, and processing history, thereby strengthening institutional accountability. However, blockchain does not automatically guarantee confidentiality or anonymity. Sensitive personal information should therefore preferably remain in

protected off-chain storage, while blockchain is used selectively for integrity verification and audit trails. Mbimbi et al. (2025), for example, propose combining zero-knowledge proofs with private blockchain technology for secure whistleblower submissions and verification, illustrating the potential of integrating distributed-ledger technology with privacy-enhancing techniques.

Second, artificial intelligence (AI) may assist in classifying, prioritizing, and analyzing large volumes of corruption reports. AI tools could identify recurring patterns, related cases, risk indicators, or unusual access patterns involving sensitive data. However, decisions concerning the credibility of allegations, investigations, or protective measures should not be fully automated. Human oversight, explainability, data minimization, procedural fairness, and mechanisms for correcting errors are essential to prevent algorithmic decisions from causing further harm.

Third, secure online reporting platforms can facilitate confidential or, where legally appropriate, anonymous reporting while reducing the need for direct contact with public officials. Encryption, access controls, multi-factor authentication, secure communication protocols, and privacy-enhancing technologies can contribute to a safer reporting environment (Di Salvo, 2020). Nevertheless, digital anonymity may still be compromised through metadata, institutional procedures, or organizational practices; therefore, technical, legal, and organizational safeguards must operate together (Berendt & Schiffner, 2021).

Fourth, big-data analytics can provide a preventive function. Properly anonymized and aggregated reporting data could help identify sectors, agencies, geographic areas, or administrative processes associated with recurring corruption risks. Digital whistleblowing systems could thus both protect individual reporting persons and generate institutional intelligence for preventive anti-corruption policies. Such use must, however, comply with strict privacy and data-protection requirements.

Vietnam has increasingly favorable conditions for applying these technologies. National policies on digital transformation, public administration reform, anti-corruption, and state restructuring provide a supportive policy environment, while national population databases, electronic identification, digital signatures, and online public-service platforms provide important

technological foundations. Increasing public familiarity with digital public services may also facilitate access to online reporting mechanisms.

However, technological availability alone cannot create public trust. Potential whistleblowers must believe that their identities will remain confidential, reports will receive meaningful follow-up, and retaliation will be addressed effectively. The EU framework accordingly treats secure reporting channels, confidentiality, acknowledgment, follow-up, feedback, and protection against retaliation as interconnected components of an effective reporting system (European Parliament & Council of the European Union, 2019).

Digitalization can potentially strengthen public confidence, reduce reporting and processing costs, improve monitoring, and enhance institutional accountability through traceable digital records. At the same time, it creates new risks, including cyberattacks against centralized databases, excessive data collection, unauthorized access, algorithmic errors, and privacy problems associated with immutable blockchain records. Therefore, digital systems should adopt a security-and-privacy-by-design approach from the outset.

A practical model for Vietnam could comprise several interconnected layers: a secure online reporting interface; privacy-preserving mechanisms for protecting identities and sensitive information; controlled case management; tamper-evident audit mechanisms; analytical tools using appropriately anonymized data; and independent oversight to monitor compliance, investigate confidentiality breaches, and provide remedies for retaliation or misuse of information.

Accordingly, the practical potential of digital technologies should be assessed not simply by technological capacity but by their integration into a coherent legal and institutional framework. International experience demonstrates that digital tools can significantly strengthen reporting mechanisms, but they cannot substitute for effective legal protection or institutional integrity (Berendt & Schiffner, 2021; European Parliament & Council of the European Union, 2019). For Vietnam, digital transformation should therefore be regarded as an opportunity for institutional reform rather than merely a technological upgrade. A secure national digital whistleblowing mechanism could improve access to reporting, strengthen confidentiality, enhance traceability, generate information for

preventive anti-corruption policies, and increase institutional accountability. With appropriate legal safeguards, cybersecurity standards, privacy-by-design principles, independent oversight, and human-centered governance, digital technology could become an important component of a modern whistleblower protection system in Vietnam's emerging model of digital national governance.

3.4. Challenges of Applying Digital Technologies to Protect Whistleblowers Reporting Corruption

Although the application of digital technologies to protect whistleblowers reporting corruption is increasingly consistent with Vietnam's national digital transformation agenda and international practices, its implementation still faces significant challenges. These challenges are not limited to legal and technological gaps but also involve social, institutional, and resource-related factors. Identifying these barriers is essential for developing a protection mechanism suited to Vietnam while progressively approaching international standards.

First, legal challenges remain a major barrier. The Law on Denunciations 2018 and its implementing regulations provide an important foundation for whistleblower protection, but they do not yet establish sufficiently detailed requirements for securely receiving and processing online denunciations. Email and online public-service portals largely represent electronic versions of traditional reporting and have not been systematically designed around anonymous reporting, advanced encryption, or tamper-evident data management. The Law on Cybersecurity 2018 and Decree No. 13/2023/ND-CP on personal data protection provide broader safeguards but do not clearly specify the data-security responsibilities of agencies receiving denunciations or sufficiently strong sanctions for disclosure or leakage of whistleblowers' information. Independent oversight also remains limited, while protective measures are primarily implemented by state agencies themselves, potentially creating conflicts of interest where officials within the same institution are involved in the allegations. Effective whistleblower protection therefore requires clear institutional responsibilities, secure reporting channels, and credible safeguards against retaliation (OECD, 2016).

Second, technological and cybersecurity challenges are significant. Although Vietnam has developed important digital infrastructure, including the national population database, VNeID, and digital signatures, cybersecurity capacity and the adoption of advanced security technologies remain uneven. A nationwide electronic whistleblowing system could become a target for cyberattacks aimed at accessing, deleting, or manipulating sensitive information. These risks may be greater at the local level, where cybersecurity capacity and technical expertise can be limited. The adoption of blockchain and AI also requires substantial investment, specialized personnel, and sustainable maintenance. As Berendt and Schiffner (2021) emphasize, technological anonymity alone cannot guarantee effective protection; technical safeguards must be combined with legal and organizational measures.

Third, social attitudes and public trust constitute another major challenge. Citizens may remain reluctant to report wrongdoing because of fear of retaliation or adverse treatment, even where legal protection formally exists. In the digital environment, concerns about identification through IP addresses, devices, metadata, or personal information may further discourage reporting. At the same time, the potential misuse of anonymous reporting for false or malicious allegations may make authorities cautious about expanding such mechanisms. Thus, technological development will have limited impact unless accompanied by greater public awareness and trust in reporting institutions.

Fourth, resource and implementation capacity remain constraints. A highly secure electronic whistleblowing system requires significant financial resources, modern infrastructure, and qualified personnel in cybersecurity and data governance. Infrastructure and technical capacity remain uneven across localities, creating a risk that digitalization may become largely formal rather than substantive. Coordination among relevant institutions, including inspection, public security, information and communications authorities, and local governments, also needs to be more systematic. Without effective coordination and sustainable resources, establishing a secure nationwide digital reporting system would be difficult.

Fifth, misuse of reporting mechanisms and the balance between competing rights present additional challenges. Anonymous digital reporting

may increase the risk of false, malicious, or personally motivated allegations. Without appropriate screening mechanisms and sanctions for abuse, excessive reporting could overload the system and reduce its ability to protect genuine whistleblowers. At the same time, confidentiality must be balanced against the procedural rights of persons subject to allegations, including their ability to understand and respond to accusations. The OECD (2016) similarly emphasizes the need to balance effective whistleblower protection with appropriate procedures for assessing and handling disclosures.

In summary, the challenges of applying digital technologies to protect whistleblowers reporting corruption in Vietnam are multidimensional, encompassing legal, technological, social, institutional, and resource-related factors. The issue is therefore not merely technological but also legal and socio-cultural. Addressing these challenges requires an integrated strategy combining legal reform, secure digital infrastructure, cybersecurity and data governance, public awareness, institutional capacity, and independent oversight. Such an approach would provide an essential foundation for developing an effective and secure whistleblower protection mechanism suited to Vietnam's emerging era of digital national governance.

3.5. Recommendations for Improving Policies and Legislation and Enhancing the Effectiveness of Digital Technology in Protecting Whistleblowers Reporting Corruption

First, the existing legal framework should be further improved. The 2018 Law on Denunciations and its implementing regulations have established an important legal foundation; however, they still lack specific provisions applicable to the digital environment. Additional provisions are needed on data confidentiality, the responsibilities of authorities receiving reports to prevent information leakage, as well as strict sanctions against acts of online retaliation against Whistleblowers Reporting. At the same time, the legal framework should be harmonized with international standards, particularly the United Nations Convention against Corruption (UNCAC) and Directive (EU) 2019/1937, thereby providing a stronger legal foundation for international integration. Article 33 of UNCAC specifically calls on States Parties to consider appropriate measures to protect persons

who report corruption-related offences in good faith and on reasonable grounds.

Second, secure digital infrastructure should be developed. Vietnam should establish secure electronic reporting platforms incorporating encryption, appropriate blockchain-based mechanisms for data integrity, and AI-assisted tools for screening and classification. These technologies can improve processing efficiency while strengthening whistleblowers' confidence in reporting. Their implementation should comply with Decree No. 13/2023/ND-CP on personal data protection and minimize risks of unauthorized access, disclosure, or misuse. Directive (EU) 2019/1937 provides a useful reference by emphasizing secure and confidential reporting channels and effective protection against retaliation (European Parliament & Council of the European Union, 2019).

Third, public awareness and implementation capacity should be enhanced. Technology alone cannot ensure effective protection if citizens remain reluctant to report corruption. Communication campaigns should promote a culture of integrity and responsible reporting, while officials should receive training in cybersecurity, data protection, and digital information management. Protection should also extend, where appropriate, to relatives and close associates of whistleblowers to reduce psychological barriers and retaliation risks, consistent with international anti-corruption standards.

Fourth, supervision, accountability, and independent evaluation should be strengthened. Digital reporting systems should be subject to regular assessment of security, confidentiality, accessibility, and effectiveness. Authorities should maintain auditable records of access, processing, and disclosure, while unauthorized access, alteration, disclosure, or misuse of reporting information should be subject to appropriate sanctions. Independent supervision and periodic evaluation are necessary to ensure that digital reporting mechanisms operate securely, transparently, and lawfully.

Fifth, inter-agency coordination and international cooperation should be enhanced. Digital whistleblower protection involves multiple actors, including receiving authorities, law enforcement agencies, data protection bodies, cybersecurity institutions, and local authorities. Clear mechanisms for information sharing, referral,

coordination, and emergency protection should therefore be established while maintaining strict confidentiality and data-protection requirements. Vietnam should also strengthen international cooperation and exchange experiences on secure digital reporting, protection against retaliation, and emerging technologies in anti-corruption efforts. Learning from international legal and technological practices would help strengthen institutional capacity and align Vietnam's whistleblower protection framework more closely with international standards.

4. Conclusion

This article has analyzed the urgency of protecting Whistleblowers Reporting corruption in the context of digital national governance, the existing legal framework, the potential applications of digital technologies, and the challenges involved. It can be seen that digital transformation creates opportunities to enhance the security, transparency, and effectiveness of protection mechanisms, while simultaneously placing greater demands on legal development, cybersecurity capacity, and efforts to overcome the social reluctance to report corruption.

In the coming period, Vietnam should continue to harmonize its legal framework with international standards, develop secure electronic reporting platforms, and strengthen independent monitoring mechanisms. These directions are important for strengthening citizens' trust, improving the effectiveness of corruption prevention and control, and building a transparent and modern Socialist rule-of-law State.

Acknowledgements

This article is developed from research conducted as part of the author's Master's thesis in Law at the School of Law, Vietnam National University, Hanoi, entitled "*The Legal Mechanism for Protecting Whistleblowers Reporting Corruption in the Private Sector: International Experiences and Implications for Vietnam*" [in Vietnamese as "*Cơ chế pháp lý bảo vệ người tố cáo tham nhũng trong khu vực tư: Kinh nghiệm quốc tế và liên hệ Việt Nam*"]. The author gratefully acknowledges the academic guidance and valuable comments provided by Associate Professor Dr. Bui Tien Dat, the thesis supervisor, which contributed to the development of the research underpinning this article.

References

- [1]. Anti-Corruption and Civil Rights Commission. (n.d.). *Clean Portal*. <https://ncp.clean.go.kr/eng/engPolicy0401.do>
- [2]. Berendt, B., & Schiffner, S. (2021). Whistleblower protection in the digital age—Why “anonymous” is not enough: From technology to a wider view of governance. *Business & Information Systems Engineering*, 63, 461–470. <https://doi.org/10.1007/s12599-021-00694-1>
- [3]. Center for Vietnamese Lexicography. (2009). *Vietnamese dictionary*. Da Nang Publishing House.
- [4]. Corrupt Practices Investigation Bureau. (2026). *E-report for corrupt conduct*. <https://www.cpib.gov.sg/e-services/e-complaint-for-corrupt-conduct/>
- [5]. Di Salvo, P. (2020). *Digital whistleblowing platforms in journalism: Encrypting leaks*. Palgrave Macmillan. <https://doi.org/10.1007/978-3-030-38505-7>
- [6]. European Parliament, & Council of the European Union. (2019). Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law. *Official Journal of the European Union*, L 305, 17–56. <https://eur-lex.europa.eu/eli/dir/2019/1937/oj>
- [7]. Lowry, P. B., Moody, G. D., Galletta, D. F., & Vance, A. (2013). The drivers in the use of online whistle-blowing reporting systems. *Journal of Management Information Systems*, 30(1), 153–190. <https://doi.org/10.2753/MIS0742-1222300105>
- [8]. Mbimbi, B., Murray, D., & Wilson, M. (2025). Preserving whistleblower anonymity through zero-knowledge proofs and private blockchain: A secure digital evidence management framework. *Blockchains*, 3(2), Article 7. <https://doi.org/10.3390/blockchains3020007>
- [9]. Melley, T. (2020). The public sphere hero: Representations of whistleblowing in U.S. culture. In K. Mistry & H. Gurman (Eds.), *Whistleblowing nation: The history of*

- national security disclosures and the cult of state secrecy* (pp. 213–242). Columbia University Press.
<https://doi.org/10.7312/mist19416-010>
- [10]. OECD. (2016). *Committing to effective whistleblower protection*. OECD Publishing.
<https://doi.org/10.1787/9789264252639-en>
- [11]. OECD. (2017). *The detection of foreign bribery*. OECD Publishing.
<https://doi.org/10.1787/8ab65bd4-en>
- [12]. Transparency International. (2024). *Corruption perceptions index 2023*.
<https://www.transparency.org/en/cpi/2023>
- [13]. United Nations. (2004). *United Nations Convention against Corruption*. United Nations Office on Drugs and Crime.
<https://www.unodc.org/unodc/en/treaties/CAC/>
- [14]. United Nations Development Programme. (2024a). *2023 Provincial Governance and Public Administration Performance Index (PAPI) report*.
<https://www.undp.org/vietnam/publications/2023-provincial-governance-and-public-administration-performance-index-papi-report>
- [15]. United Nations Development Programme. (2024b, April 2). *According to the 2023 PAPI survey, citizens report improvements in local anti-corruption efforts and e-governance amid concerns about transparency and the economic situation*.
<https://www.undp.org/vi/vietnam/press-releases/theo-khao-sat-papi-2023-nguoi-dan-cho-biet-co-cai-thien-trong-no-luc-phong-chong-tham-nhung-va-quan-tri-dien-tu-o-dia-phuong>
- [16]. United Nations Office on Drugs and Crime. (2015). *Resource guide on good practices in the protection of reporting persons*. United Nations.
https://www.unodc.org/documents/corruption/Publications/2015/15-04741_Person_Guide_eBook.pdf
- [17]. Vu Cong Giao, & Tran Thuy Duong. (2024). Further improving the legal mechanism for protecting whistleblowers reporting corruption in Vietnam. *Journal of Procuracy and Judicial Science*, 7(79).