DATA ETHICS IN THE DIGITAL ECONOMY: BALANCE BETWEEN PRIVACY AND BUSINESS INTERESTS

PhD. Chu Thi Hong Hai*

Abstract: ***This study analyzes Decree 13/2023/ND-CP and business practices in Vietnam to propose a sustainable data governance model that balances individual privacy and business interests in the digital economy. Employing a qualitative methodology, the results identified three main barriers: technical limitations, organizational culture factors, and data commercialization pressures, along with significant differences in compliance levels across industries. Accordingly, the study proposes four groups of strategic solutions and contributes to the theoretical foundation of data ethics, while also providing effective policy recommendations for Vietnamese businesses.***

• Keywords: *data ethics, privacy, personal data protection, data governance, digital economy.*

Date of receipt: 20th Oct, 2025
Date of delivery revision: 26th Oct., 2025
Date of receipt revision: 05th Nov., 2025
Date of approval: 25th Nov., 2025

DOI: https://doi.org/10.71374/jfar.v25.i6.10

1. Introduction

In the context of the digital economy, personal data is an important asset that fosters innovation and creates competitive advantage, especially in e-commerce and FinTech (OECD, 2021). However, the innovation and competitive advantage of personal data e-commerce and FinTech directly clashes with the right to privacy protected under Article 21 of the 2013 Vietnamese Constitution, and global frameworks like the GDPR, CCPA, and PDPA (European Commission, 2020; California Legislative Information, 2018; PDPC Singapore, 2021). Though Decree 13/2023/ND-CP marks a legal achievement (Government of Vietnam, 2023), gaps in enforcement and oversight fraught with a lack of public trust, a vital component of the resilience in a digital ecosystem, continue to exist (Regulatory Frameworks, 2023; Taylor, 2021). Governance issues resulting from lack of transparency, excessive focus on data monetization, and insufficient investment in security face Vietnamese organizations (Viettel Cyber Security, 2023).

Trust needs to be established and fostered by incorporating data ethics grounded on transparency, equity, accountability, and a right for every human to be treated fairly (OECD, 2021). Ethical data governance that upholds compliance with legal regulation and fosters innovation stands a better chance of performing better internationally (PDPC Singapore, 2021). As Vietnam becomes more involved in global value chains, it is important to make data ethics a regulatory standard and a strategic necessity (Taylor, 2021; Westin, 1967). Privacy should not be treated as absolute; it can be balanced with legitimate data use through ethical adaptive governance reasoning.

2. Literature review

2.1. Theoretical framework

Data Ethics focuses on the principles and values responsible data-handling practices that build trust in society, going beyond compliance with the law (Floridi & Taddeo, 2016). Ethical data governance as proposed by OECD (2021) requires accountability through internal audits, privacy shield via protective technologies such as encryption and AI, and trust transparency in corporate policies. These practices embed trust into corporate strategy, fostering long-term competitiveness.

Institutional Theory (DiMaggio & Powell, 1983) explains organizational actions through the lens of coercive legal mandates (e.g., Decree 13/2023), mimetic pressures from industry leaders, and normative pressures from consumers and civil society. These pressures compel firms to go beyond the minimum regulatory thresholds in order to maintain reputation and stakeholder trust.

Stakeholder Theory (Freeman, 1984) supports engaging all stakeholders, which in this case includes the consumers, regulators, and the general public, as a reason for open engagement that alleviates tension between economic aims and the invasion of privacy. Additionally, Westin (1967) in his “privacy as control” model suggests that by providing the public

** Banking Academy; email: haict@hvnh.edu.vn*

with considerable control over personal information improves the acceptability of data practices.

Enterprise Data Governance based on OECD (2021) applies the ethical and institutional aspects through defined workflows, delineated structures of responsibility, and anticipatory risk mitigation. This consolidated strategy is useful for the organizations because it allows them to turn compliance in to a competitive advantage.

2.2. Literature review

The digital economy is growing quickly, and personal data is now a key factor in how well businesses work and how competitive they are (OECD, 2021). A lot of research has been done on legal and technical security issues, but there has not been much research on data ethics in corporate governance, especially in developing countries like Vietnam. This gap underscores the need for an integrated framework that aligns ethical principles, institutional mandates, and business interests to reconcile privacy protection with effective data utilization.

Data governance is put at risk by security breaches, cybersecurity incidents, and loss of sensitive or confidential information, which in turn erodes consumer trust and has enduring financial ramifications (Cybersecurity Report, 2023). Over 60% of breaches, as explored by Shackelford (2020), stem from internal or human error, and, as Ambore (2021) finds, lack of awareness of data governance frameworks and inconsistent enforcement of organizational policies and set rules are major contributing factors. Therefore, governance involves rigorous legal mechanisms and frameworks, comprehensive compliance policies, policies and procedures, and organizational compliance culture.

Legal instruments with concrete enforcement mechanisms, for example the EU's GDPR (European Commission, 2020), California's CCPA (California Legislative Information, 2018), and Singapore's PDPA (PDPC Singapore, 2021), which demand for accountability and compliance transparency, also impose severe fines. In Vietnam, the legal framework includes the 2015 Civil Code, the 2018 Law on Cyber Security, Decree 13/2023/ND-CP on data safeguarding, the Decision 06/QD-TTg (2022) on population data, and Circular 24/2022/TT-BTTTT on the protection of IT systems. Vietnam, on the other hand, is missing primary governance structures, strong frameworks for data commercialization, or reliable ways to check if organizations are following data ethics (Regulatory Frameworks, 2023).

Scholars are still focusing on the technical and legal aspects of data privacy (Floridi & Taddeo, 2016; Ambore, 2021). There is a lack of thorough research on data privacy ethics in Vietnamese businesses, particularly in relation to compliance with Decree 13/2023. As a result, no one has attempted to apply ethical, institutional, and stakeholder theory along with Westin's (1967) "privacy as control" framework to examine the management and ethical obligation oversight ecosystem of Vietnamese businesses. In addition, while AI and blockchain are esteemed technologies, their adoption is hampered by severe cost and technical capability constraints, as well as reliance on foreign firms for small and medium-sized enterprises (SMEs) in Vietnam.

This paper fills these gaps by analyzing the ethical challenges of data governance in Vietnam, evaluating the regulatory and trust implications of Decree 13/2023, and proposing solutions to enhance privacy protection while facilitating data use. The primary objective is to construct a Vietnamese contextual framework for institutional and digital elements by proposing an adaptable data governance model that is transparent, accountable, and sustainable.

2.3. A comparison among data protection policies of Vietnam and some developed regions

Table 1: A comparison among data protection policies of Vietnam and three developed regions

Criteria	GDPR (EU, 2018)	CCPA (US, 2018)	PDPA (Singapore, 2012; amended 2020)	Decree 13/2023 (Vietnam)
Scope of Application	Entities processing EU citizens' data	Firms with >$25M revenue or handling CA data	All data processors in SG	Entities handling VN citizens' data, domestic or foreign
Individual Rights	Access, correction, erasure, objection, portability	Refuse data sale, access, deletion	Access, correction, consent withdrawal, portability	Access, correction, deletion, restriction, portability
Enforcement Mechanism	Fines up to 4% of global turnover	Fines up to $7,500/ violation	Up to 10% turnover or 1M SGD	Warnings, fines, criminal liability, compensation
Supervisory Authority	EDPB (independent)	California Attorney General	PDPC (independent	Ministry of Public Security (no independent body)
Sensitive data	Strictly defined and protected	Not clearly defined; disclosure required	Clear handling policies	Defined; lacks detailed guidance
Cross-border Transfer	Allowed to GDPR-compliant jurisdictions	No strict limits; transparency required	Risk-based safeguards mandatory	Notification required; adequacy not clearly enforced
Accountability & Registration	DPO, records, compliance proof	Source disclosure, verification mechanisms	DPO, audits, notifications	Internal policies required; limited enforcement

Source: Author's comparative compilation

Compared to the GDPR, CCPA, and PDPA, three key shortcomings of Vietnam's Decree 13/2023/ND-CP remain: (i) the lack of an independent supervisory authority; (ii) weak enforcement and limited sanctions; and (iii) vague regulations on sensitive data and cross-border transfers.

3. Research methods

3.1. Research approach and data collection

To assess data governance and ethics in Vietnamese businesses, this study employed a qualitative methodology combining document analysis, case studies, and expert interviews. Due to limitations in large-scale survey data, the qualitative approach was chosen to gain deeper insights into stakeholder perspectives and implementation practices.

Data were collected from two primary sources. Secondary materials included industry reports, governmental regulations, and prior academic studies. Primary data were gathered through interviews with ten professionals, each with at least five years of experience in data security or policy, representing sectors such as FinTech, telecommunications, e-commerce, and digital health.

Fifteen businesses with substantial data operations were selected based on their exposure to Decree 13/2023/ND-CP and the presence of either data protection policies or previous data breach incidents. Covering the period from 2020 to 2024, the study explores governance challenges, ethical risks, and compliance behaviors.

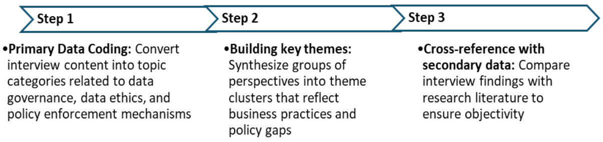
Guided by the OECD data ethics model (2021), a multifaceted analytical lens was applied to examine institutional, ethical, and operational factors. To ensure objectivity, standardized interview protocols, double-coding techniques, and participant validation procedures were implemented.

3.2. Data analysis methods

We used content and topic analysis to look for important themes in the data from expert interviews. Content analysis looked at legal papers, industry reports, and academic studies to find gaps in data ethics norms and policies. Thematic analysis used information from case studies and interviews to find patterns and suggest ways to fix problems. These techniques were based on the OECD's data ethics model (2021) and made sure that the recommendations for sustainable data governance in Vietnam were founded on facts.

The data analysis process consists of three steps:

Figure 3. Data analysis process



Step 1

- **Primary Data Coding:** Convert interview content into topic categories related to data governance, data ethics, and policy enforcement mechanisms

Step 2

- **Building key themes:** Synthesize groups of perspectives into theme clusters that reflect business practices and policy gaps

Step 3

- **Cross-reference with secondary data:** Compare interview findings with research literature to ensure objectivity

The practical assessment framework is based on the OECD Data Ethics Model (2021) and is designed to make simpler to compare and analyze data across different industries. This assists in find solutions that are precisely for Vietnamese businesses.

3.3. Ensuring reliability and objectivity

To ensure objectivity, the study employed three data validation strategies: (1) data triangulation through cross-verification of documents, cases, and interviews; (2) independent expert review of collected data; and (3) transparency in research design, including disclosure of sampling criteria and analytical methods. Additionally, interview tools were standardized, data were transcribed and double-coded, and findings were confirmed with participants to minimize bias and enhance reliability.

4. Research results and discussion

4.1. Results on data governance and data ethics in enterprises in Vietnam

The study notes that compliance with personal data protection regulations in Vietnamese enterprises is currently strongly influenced by three institutional factors according to the theory of DiMaggio & Powell (1983): coercive pressure (from the state), imitative pressure (from pioneering enterprises) and normative pressure (from social expectations). Although Decree 13/2023/ND-CP has laid a relatively clear legal foundation, implementation still varies widely across industries and enterprise sizes, reflecting differences in ethical awareness, internal capacity and the level of commitment to data culture.

Compliance levels and industry differences

A sector-by-sector examination shows that different industries have very different levels of compliance with data protection laws. In telecommunications and FinTech, companies follow the rules very closely. This is mostly because government agencies like the State Bank and the Ministry of Information and Communications are quite strict about following the rules. Many companies in these fields have started using international standards like ISO/IEC 27001, AI to keep an eye on data, and frequent internal audits (IBM Security, 2022).

On the other hand, the e-commerce industry is less stable. Major platforms like Shopee, Tiki, and Lazada have created formal data protection policies. However, most small and medium-sized businesses (SMEs) don't have the resources to do this, so they just copy what the big companies do, which means that compliance is mostly superficial (Viettel Cyber Security, 2023).

The digital health sector has the lowest levels of compliance. This is because there are no standardized data governance procedures or industry-specific norms. Only 25% of private healthcare providers have explicit privacy policies.

Generally, more than half of Vietnamese businesses still don’t have a separate department for data security. This disparity makes enforcement measures far less effective and makes accountability weaker, which is one of the main parts of good data governance (OECD, 2021).

The challenge of balancing privacy and business interests

Utilizing the OECD Data Ethics Model (2021), the study indicates that organizations with robust data governance exhibit several essential traits. This encompasses a dedication to information transparency, robust accountability procedures, and significant investment in modern security technologies elements that strongly correspond with the theoretical foundations of the study. Nonetheless, substantial obstacles persist in hindering the wider implementation of ethical data governance in Vietnam.

Financial limitations constitute a significant obstacle, especially for small and medium-sized firms (SMEs), who frequently find it challenging to adopt expensive technology like AI and blockchain. Conversely, huge organizations such as Viettel or Momo might provide annual budgets between USD 500,000 and over one million for data protection systems. The ongoing lack of openness in data management is also concerning: over 60% of companies fail to grant users the ability to access, modify, or delete their data, which clearly contravenes Westin’s (1967) “Privacy as Control” paradigm.

Moreover, the financial impetus to capitalize on data has compelled some companies to transgress the limits of user consent, frequently disseminating personal data to third parties without explicit agreement. This compromises data ethics standards and diminishes public trust (Floridi & Taddeo, 2016). The lack of independent oversight and robust sanctions promotes reactive compliance tactics instead of fostering substantial ethical frameworks.

4.2. Solutions to balance privacy and business interests

Improving the legal framework and enforcement mechanism

Although Decree 13/2023/ND-CP has laid the groundwork for personal data protection in Vietnam, substantial regulatory gaps remain when compared to more mature frameworks such as the GDPR in the European Union and the PDPA in Singapore (European Commission, 2020; PDPC Singapore, 2021). These deficiencies limit the effectiveness of current legislation and weaken incentives for compliance.

To strengthen enforcement and foster a culture of accountability, a set of institutional and regulatory enhancements is imperative. First, the establishment of an independent supervisory authority, such as a National Data Protection Commission. This body would be responsible for monitoring compliance, conducting audits, issuing guidance, and imposing sanctions (OECD, 2021). Second, sanction mechanisms must be reinforced through the introduction of administrative fines proportional to enterprise revenue, following deterrent models embedded in the GDPR and PDPA. Such measures would elevate the cost of non-compliance and provide concrete incentives for proactive data protection. Third, the regulatory framework should clearly define sensitive data categories, particularly financial, medical, and biometric information, and mandate enhanced security safeguards to mitigate risks associated with misuse or breaches. Finally, to regulate international data transfers, Vietnam should adopt an adequacy-based approach aligned with GDPR principles, permitting cross-border flows only to jurisdictions with comparable levels of data protection. This would ensure the integrity of outbound data streams and facilitate greater international trust in Vietnam’s digital ecosystem.

KPI to evaluate effectiveness: ≥ 60% of businesses issue clear security policies by 2027.

Strengthen data monitoring and auditing

A robust legal framework must be supported by a comprehensive monitoring and auditing system to ensure that compliance transcends mere adherence to regulations. To accomplish this, it is recommended that some policy modifications be implemented to enhance institutional efficacy and public trust.

First, big companies that work with a lot of data, like FinTech, telecoms, and e-commerce, should have to have annual data audits, like financial audits, to find weaknesses and make sure security requirements are followed. Secondly, corporations must to publicly provide compliance reports detailing their methods for collecting, utilizing, and safeguarding personal data. This strategy enhances organizational accountability while also fostering greater confidence and trust in digital services among individuals. Third, enhancing international collaboration through participation in multilateral agreements and treaties that safeguard data is essential. This level of engagement facilitates the adoption of global best practices and enables collaborative efforts across borders to investigate and address data privacy issues.

KPI to evaluate effectiveness: ≥ 40% of FinTech and e-commerce businesses audit data annually.

Improving security capabilities in enterprises

Most Vietnamese businesses, especially SMEs, have limited resources and data security expertise. Focusing only on sanctions without supporting policies can lead to reactive responses, reducing overall effectiveness. Solutions that need to be implemented include:

Solution	Describe	Implementing unit
Tax incentives	Tax breaks for businesses that invest in data security.	Ministry of Finance
Human resource training	Organize in-depth training courses on data management.	Ministry of Information and Communications & Business Associations
Technology application support	Support businesses to access AI, Blockchain, MFA to enhance security.	Ministry of Industry and Trade & Ministry of Science and Technology

KPI for evaluating effectiveness: ≥ 50 security training courses organized/year by 2027.

Controlling the commercialization of personal data

The collection, use, sharing and sale of personal data are not yet strictly controlled, potentially posing a risk of privacy infringement and damaging social trust (Floridi & Taddeo, 2016). Proposed groups of solutions:

Solution	Describe	Implementing unit
Empowering individuals to opt-out of personal data sales	Enterprises must provide users with the option to refuse the sharing of their personal data	Data Protection Authority, Ministry of Information and Communications
Enhancing transparency in data collection processes	Enterprises are required to publicly disclose how personal data is collected and used	Ministry of Industry and Trade, Ministry of Information and Communications
Periodic audits of data usage	Mandatory audits must be onducted to assess the level of corporate compliance with data protection regulations	Data Protection Authority

KPI to evaluate effectiveness: ≥ 70% of businesses provide an "opt-out" feature for users in 2027.

Building a sustainable data governance ecosystem

Creating a long-lasting data governance ecosystem based on confidence from society and supported by the integration of legal, technological, and educational elements is necessary for good data security. The effectiveness of this type of ecosystem depends on a number of aspects that are all linked together. For governance solutions to work in the real world and last, policy, technology, and education must all be in sync. Second, building strong ties between the public and private sectors is important for effective implementation because it makes compliance and flexibility easier when the government, businesses, and other stakeholders work together. Third, policy frameworks need to be flexible and fit the situation in Vietnam, rather than just copying international models without making any changes. It is suggested that at least 50% of large firms perform annual social trust assessments to provide a standard for measuring how well ethical data governance practices are working and how mature they are.

5. Conclusion

This paper investigates the conflict between privacy and commercial interests in the context of Vietnam's digital economy focusing on the implementation of Decree 13/2023. Aside from the legal developments made, there still exist three previously discussed barriers that continue to hinder the creation of a sustainable ethics framework for data in Vietnam.

This research enhances theoretical understanding and practical application by refining the conceptual framework of data governance in developing environments and providing pragmatic policy recommendations for Vietnamese regulators and enterprises. When applied cohesively, proposed solutions can cultivate a reliable and competitive digital ecosystem, in accordance with global data governance standards.

References:

Ambore, T. (2021). Data security challenges in the digital economy: Human factors and policy implications. Journal of Cybersecurity Studies , 14(2), 45–63.

California Legislative Information. (2018). California Consumer Privacy Act (CCPA) . https://oag.ca.gov/privacy/ccpa

Cybersecurity Report. (2023). Global data assessments and security threats in 2023. International Cybersecurity Review .

DiMaggio, P.J., & Powell, W.W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review , 48(2), 147–160. https://doi.org/10.2307/2095101

European Commission. (2020). General Data Protection Regulation (GDPR).
https://gdpr-info.eu/

Freeman, R.E. (1984). Strategic management: A stakeholder approach . Boston: Pitman.

IBM Security. (2022). Cost of a Data Breach Report 2022
https://www.ibm.com/reports/data-breach

Government of Vietnam. (2023). Decree 13/2023 on personal data protection . Hanoi: Government of Vietnam.

Ministry of Information and Communications. (2022). Circular No. 24/2022/TT-BTTTT regulating the protection of personal data in information systems. Hanoi: Ministry of Information and Communications.

Organization for Economic Co-operation and Development (OECD). (2021). OECD digital economy outlook 2021 . OECD Publishing.
https://www.oecd.org/en/publications/development-co-operation-report-2021_ce08832f-en.html

PDPC Singapore. (2021). Personal Data Protection Act (PDPA) Guidelines.
https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act

National Assembly of the Socialist Republic of Vietnam. (2018). Law on Cyber Security No. 24/2018/QH14 . Hanoi: Office of the National Assembly.

Regulatory Frameworks. (2023). Data privacy regulations and enforcement mechanisms in Southeast Asia. Asian Legal Review , 9(1), 112–135.

Shackelford, S.J. (2020). Human error and data security: The overlooked risk in cybersecurity governance. Journal of Information Policy , 10, 234–256.

Taylor, L. (2016). The ethics of big data as a public good: which public? Whose good? Philosophical Transactions of the Royal Society A, 374(2083), 20160113.
https://doi.org/10.1098/rsta.2016.0113

Westin, A. F. (1967). Privacy and freedom . New York: Athens.