Artigo original

http://dx.doi.org/10.18623/rvd.v23.5186

GOVERNANCE OF CONSUMERS' PERSONAL DATA IN E-COMMERCE IN VIETNAM

GOVERNANCA DE DADOS PESSOAIS DE CONSUMIDORES NO COMERCIO ELETRONICO NO VIETNA

Article received on: 11/4/2025
Article accepted on: 2/6/2026

Luong Tuan Nghia*
*University of Law, Vietnam National University, Hanoi, Vietnam
Orcid: https://orcid.org/0009-0000-8122-8688
nghia.thudohanoi@gmail.com

Nguyen Minh Tuan*
*University of Law, Vietnam National University, Hanoi, Vietnam
Orcid: https://orcid.org/0009-0007-0650-986X
tuannm@vnu.edu.vn

The authors declare that there is no conflict of interest

Abstract
This article examines the governance of consumers' personal data in Vietnam's e-commerce sector. It argues that the rapid expansion of the country's digital economy has intensified the collection, processing, and circulation of personal data across online platforms, thereby increasing risks of misuse, unauthorized disclosure, and inadequately controlled cross-border transfers. Based on doctrinal analysis of Vietnamese law and comparative engagement with the European Union's General Data Protection Regulation, the article shows that Vietnam is moving from a fragmented privacy-protection approach toward a more structured model of data governance. Nevertheless, important weaknesses remain, including regulatory inconsistency, limited enforcement capacity, fragmented supervisory arrangements, and insufficiently effective mechanisms for the exercise of data-subject rights. The article concludes by proposing legislative and institutional reforms designed to strengthen platform accountability, improve the coherence of sanctioning mechanisms, and enhance consumer trust in the digital marketplace.

Keywords: Consumer Protection. Data Governance. E-Commerce. Personal Data. Vietnam.

Resumo
Este artigo examina a governanca de dados pessoais de consumidores no setor de comercio eletronico no Vietna. O estudo parte do pressuposto de que a rapida expansao da economia digital vietnamita intensificou a coleta, o tratamento e a circulacao de dados pessoais em plataformas digitais, ampliando riscos de vazamento, uso indevido e transferencia internacional sem controle suficiente. Com base em analise dogmatica do direito vietnamita e em dialogo comparado com o Regulamento Geral de Protecao de Dados da Uniao Europeia, o artigo demonstra que o Vietna avanca de um modelo fragmentado de tutela da privacidade para um regime mais estruturado de governanca de dados. Apesar desse progresso, persistem problemas de coerencia normativa, capacidade fiscalizatoria, definicao de competencias sancionatorias e efetividade dos direitos de controle do titular. Ao final, o texto propoe aperfeicoamentos legislativos e institucionais destinados a reforcar a responsabilizacao das plataformas, a efetividade das sancoes e a confianca dos consumidores no mercado digital.

Palavras-chave: *Comercio Eletronico. Dados Pessoais. Governanca de Dados. Protecao do Consumidor. Vietnam.*

1 INTRODUCTION

Vietnam's digital economy has expanded rapidly in recent years, and this transformation has made the protection of personal data an increasingly significant legal and regulatory issue. The concern is particularly acute in the field of e-commerce, where platforms routinely collect, store, analyze, and exchange large volumes of consumer information in order to facilitate transactions, personalize services, and optimize commercial strategies.

In response, Vietnam has adopted a more structured legal approach to the governance of personal data. The legal framework now combines general rules on electronic transactions, specific provisions on personal data protection, and administrative sanctioning mechanisms applicable to digital commerce. This evolution reflects a broader shift from a narrow focus on consumer information confidentiality toward a more comprehensive conception of personal data governance in the digital marketplace.

At the same time, the growth of e-commerce has created new regulatory pressures. Consumer data has become a valuable economic asset, but it has also become more vulnerable to unlawful collection, uncontrolled sharing, fraudulent exploitation, and cross-border transfer without sufficient oversight. These developments raise difficult questions concerning the adequacy of existing legal safeguards, the distribution of regulatory responsibilities, and the practical enforceability of statutory rights.

Against this background, this article examines the principal legal challenges involved in protecting consumers' personal data in Vietnam's e-commerce environment, assesses the extent to which the new legal framework responds to those challenges, and proposes reforms aimed at improving coherence, enforceability, and institutional accountability. By situating Vietnam’s recent legislative developments within the broader challenges of platform-based data governance, this article contributes to ongoing debates on how emerging digital economies can strengthen consumer protection without undermining regulatory coherence or market development.

Vietnam’s recent legal development should also be understood in light of two important statutes enacted in 2025. The Law on Personal Data Protection marks the transition from decree-based regulation to a formal statutory framework with broader

rights and obligations, while the Law on Artificial Intelligence introduces a risk-based governance model relevant to digital platforms that rely on automated profiling, recommendation systems, and targeted advertising. Together, these laws indicate that consumer data governance in e-commerce can no longer be understood solely as a matter of confidentiality, but increasingly as a matter of platform accountability, transparency, and technologically mediated decision-making.

2 LITERATURE REVIEW AND THEORETICAL BACKGROUND

Contemporary scholarship increasingly treats personal data not merely as an extension of privacy, but also as an economic and regulatory object situated at the intersection of market power, informational asymmetry, and technological infrastructure. In data-driven markets, personal data enables profiling, targeted advertising, behavioral prediction, and product optimization, thereby becoming a strategic asset for digital enterprises (MAYER-SCHONBERGER; CUKIER, 2013). This shift has important legal implications, because the governance of personal data is no longer confined to protecting individual privacy in a narrow sense; it now also concerns the regulation of digital markets, the allocation of informational power, and the accountability of platform-based business models.

From a comparative legal perspective, the European Union's General Data Protection Regulation (GDPR) remains one of the most influential reference points for national data-protection frameworks. Its normative structure is built around principles such as lawfulness, transparency, purpose limitation, data minimization, storage limitation, integrity, and accountability, while also strengthening the procedural and substantive rights of data subjects (DE HERT; PAPAKONSTANTINOU, 2016). The influence of the GDPR has extended far beyond the European Union, shaping legislative developments in a growing number of jurisdictions that have adopted or revised comprehensive personal data protection laws under its conceptual and regulatory influence (GREENLEAF, 2021). In this sense, contemporary data governance is increasingly shaped by transnational normative convergence, even where national legal systems continue to differ in institutional design and enforcement capacity.

At the same time, digital markets are characterized by the constant movement of personal data across organizational and territorial boundaries. Cross-border data flows have therefore become one of the most complex issues in modern data governance, since personal data routinely circulates through transnational digital infrastructures that do not fit neatly within the jurisdictional boundaries of a single state (KUNER, 2013). This complexity is particularly relevant in platform-based economies, where data may be collected in one jurisdiction, processed in another, and monetized across multiple markets simultaneously. As a result, questions of sovereignty, regulatory reach, and enforceability have become central to contemporary debates on personal data governance.

The platform economy also introduces a structural imbalance between consumers and digital intermediaries. Platforms possess superior technical capacity, contractual leverage, and informational control, whereas individual users frequently lack meaningful knowledge about the downstream use, sharing, and commercial exploitation of their data. This asymmetry justifies a stronger regulatory emphasis on transparency, valid consent, auditability, and effective redress mechanisms. In this context, the governance of personal data must be understood not only as a matter of individual rights, but also as a question of institutional design and market regulation.

Within Vietnam, academic discussion has expanded in parallel with recent legislative reforms. Even so, much of the existing debate still concentrates on privacy in general terms or on cybersecurity regulation. The specific governance of consumers' personal data within e-commerce ecosystems remains comparatively underexplored, particularly in relation to platform accountability, cross-border data transfers, and the coherence of enforcement mechanisms. This article addresses that gap by connecting doctrinal analysis of Vietnamese law with a broader comparative and governance-oriented framework, situating Vietnam's recent reforms within both the structural logic of platform capitalism and the wider global evolution of data protection law.

Recent regulatory debates increasingly emphasize the interaction between personal data governance and artificial intelligence regulation. AI systems rely heavily on large datasets for training and operation, which raises new legal questions concerning transparency, algorithmic accountability, and data protection compliance. The Law on Artificial Intelligence of Vietnam (2025) reflects this emerging regulatory trend by introducing risk-based classification of AI systems, transparency obligations, and

safeguards for affected persons. These developments suggest that personal data governance in digital markets cannot be analysed in isolation from broader regulatory frameworks governing algorithmic decision-making and platform technologies.

3 RESEARCH METHODOLOGY

This study adopts doctrinal legal research as its principal method and combines it with comparative legal analysis. The doctrinal component is used to interpret the structure, scope, and internal coherence of Vietnam's legal framework governing personal data in e-commerce. Particular attention is paid to the interaction between constitutional protections, civil-law safeguards, administrative sanctions, and the newly enacted data-protection legislation.

The article also employs comparative analysis by using the European Union's GDPR as an interpretive benchmark. The purpose of this comparison is not to assume regulatory equivalence, but to clarify where Vietnam's framework converges with internationally recognized standards and where important divergences remain, especially in relation to supervisory independence, data-subject control, and sanctioning design.

In addition, the article relies on secondary materials, including official policy reports and regulatory documents concerning the development of Vietnam's e-commerce market and the enforcement of digital-market rules. These materials provide empirical context for assessing the practical significance of the legal issues discussed in the article (E-COMMERCE AND DIGITAL ECONOMY AGENCY, 2023; GENERAL DEPARTMENT OF MARKET SURVEILLANCE, 2023; GENERAL DEPARTMENT OF MARKET SURVEILLANCE, 2024).

4 RESULTS AND DISCUSSION

4.1 Challenges in protecting consumer personal data on e-commerce platforms

Vietnam’s e-commerce market has expanded at remarkable speed, and official reports indicate that it is now among the fastest-growing digital markets globally (E-COMMERCE AND DIGITAL ECONOMY AGENCY, 2023). This rapid expansion has

increased not only the economic value of consumer personal data, but also its exposure to misuse, unauthorized disclosure, and regulatory non-compliance. In practice, data generated through online shopping, mobile applications, and integrated digital services may be collected, processed, and shared across multiple entities, including e-commerce platforms, payment intermediaries, logistics providers, and advertising partners. As a result, consumer personal data is no longer handled within a single, easily identifiable transactional relationship, but within a dispersed and interconnected digital ecosystem.

This environment creates several layers of risk. First, consumers may be exposed to unauthorized disclosure, unlawful collection, or secondary use of their data beyond the purpose originally communicated to them. Second, the complexity of integrated digital ecosystems makes it difficult for users to determine which entity actually controls their data, which entity merely processes it, and which entity should bear responsibility when a violation occurs. Third, personal data breaches in the e-commerce environment may expose consumers to fraud, impersonation, unwanted commercial targeting, and other forms of digital harm. The legal significance of these risks lies not only in the possibility of data leakage itself, but also in the increasing asymmetry between platforms that control data flows and consumers who have only limited visibility over the downstream use of their information.

A particularly serious challenge concerns the practical effectiveness of deletion and control rights. Pursuant to Clause 5, Article 16 of Decree No. 13/2023/ND-CP of the Government on Personal Data Protection, and later reflected in Clause 5, Article 8 of the Personal Data Protection Law (2025), data subjects are entitled to request protective measures against unlawful processing, while the broader statutory framework also imposes obligations relating to correction, storage, and deletion. In formal terms, this provides an important layer of legal protection. In practice, however, the exercise of these rights remains difficult to verify in the e-commerce environment, particularly where consumer data has already been distributed across multiple service providers or incorporated into platform-based operational systems. This means that the existence of statutory rights does not automatically guarantee effective consumer control where data flows are technically complex and institutionally fragmented.

Cross-border data transfer presents an additional and particularly difficult regulatory challenge. Under Articles 24 and 25 of Decree No. 13/2023/ND-CP of the

Government on Personal Data Protection, organizations transferring personal data abroad must prepare transfer-impact documentation and comply with procedural safeguards. This difficulty becomes even more acute in cases involving cross-border data transfers, where personal data may move through transnational platform infrastructures that are not easily subjected to a single national enforcement framework (KUNER, 2013). In practice, once data has been transferred into transnational digital systems, effective oversight becomes significantly more complex, and domestic authorities may face serious obstacles in detecting, tracing, and remedying violations in a timely manner. This problem is especially acute in the context of large cross-border platforms, where data may be continuously synchronized across multiple jurisdictions and integrated into broader commercial ecosystems beyond the immediate reach of domestic regulators.

4.2 Structural limitations of Vietnam's legal framework on the protection of consumers' personal data

Vietnamese law now recognizes the protection of personal data as part of a broader legal framework designed to safeguard privacy, dignity, and informational autonomy. At the constitutional level, Article 21 of the Constitution of the Socialist Republic of Vietnam (2013) affirms the inviolability of private life, personal secrets, and family secrets, while also recognizing the right of individuals to protect their honor and reputation. At the private-law level, Clause 1, Article 9 and Article 38 of the Civil Code (2015) reinforce these guarantees by requiring consent for the collection, storage, use, and disclosure of information linked to personal and family secrecy. These provisions establish an important normative foundation, but they remain general in nature and were not originally designed to address the technical and institutional complexities of platform-based data processing in the digital economy.

Before the adoption of a dedicated statute, Vietnam regulated this field through a fragmented body of rules scattered across e-commerce law, consumer protection law, cybersecurity regulation, and administrative sanctioning instruments. Decree No. 52/2013/ND-CP of the Government on E-commerce relied on the older concept of “personal information” and imposed confidentiality obligations on traders and e-commerce platforms. Decree No. 85/2021/ND-CP later amended that framework,

including revisions to prohibited acts in e-commerce. However, the principal weakness of this earlier model was not merely dispersion, but regulatory layering without sufficient harmonization. Successive amendments were introduced on top of older provisions, while related sanctioning rules were not systematically revised at the same pace. As a result, the legal framework developed in a piecemeal manner, producing overlaps in terminology, inconsistencies in scope, and uncertainty as to which conduct was prohibited, which authority was competent, and which sanctioning rule should apply.

The Personal Data Protection Law (2025) also introduces clearer rules governing cross-border data transfer, impact assessment obligations, and enhanced administrative sanctions for violations. In this respect, Vietnam's legislative reform is not an isolated development, but part of a wider global movement toward more comprehensive personal data protection regimes influenced by the regulatory architecture of the GDPR (GREENLEAF, 2021). Against this broader background, Article 4 of the Personal Data Protection Law (2025) recognizes core rights of data subjects, including the rights of access, consent, withdrawal of consent, objection, restriction of processing, and deletion. Article 14 and Article 15 further regulate obligations concerning the protection, processing, and disclosure of personal data. At the institutional level, Clause 1, Article 23 and Clause 4, Article 23 assign supervisory functions to the specialized authority responsible for personal data protection, while Point (a), Clause 1, Article 33 confirms its competence to receive notifications and enforce compliance measures. In formal terms, this is a significant legislative advance. Yet the shift from a fragmented regime to a statutory framework does not, by itself, resolve the underlying problems of regulatory coherence and enforcement design.

The first major limitation of the current framework lies in the gap between the recognition of rights and the practical enforceability of those rights. Although Article 4 of the Personal Data Protection Law (2025) grants data subjects a relatively broad set of control rights, the law is much less precise on the operational obligations imposed on platforms in implementing those rights in complex digital environments. For example, while the law recognizes rights of access, deletion, and objection, it does not yet provide a sufficiently detailed procedural architecture governing verification, response timelines across multiple data intermediaries, documentation of compliance, or evidentiary burdens when disputes arise. In the context of e-commerce, where data may be simultaneously

processed by platforms, payment intermediaries, logistics providers, and advertising partners, this omission is not merely technical. It weakens the real exercise of statutory rights because a legal entitlement without a clear enforcement pathway can easily become symbolic rather than effective.

A second weakness concerns the incomplete alignment between substantive data-protection norms and the administrative sanctioning regime. Clause 4, Article 8 of the Personal Data Protection Law (2025) provides that the maximum fine for organizations violating cross-border data-transfer rules may reach 5 percent of the preceding year's revenue, while Clause 5, Article 8 establishes additional sanctioning formulas for other categories of violation. On paper, this reflects a stronger deterrent orientation. In practice, however, sanctions in the e-commerce sector still rely heavily on Decree No. 98/2020/ND-CP of the Government on administrative sanctions in commercial activities, the production and trading of counterfeit and prohibited goods, and the protection of consumer rights. The problem is therefore one of normative disconnect: the new law introduces a stronger data-protection logic, but enforcement still depends in significant part on an older decree drafted for a broader commercial-regulation context rather than for the structural realities of digital data governance. This disconnect creates a risk that the legal system will recognize modern data rights while enforcing them through outdated or incomplete sanctioning tools.

One illustrative inconsistency concerns the relationship between Clause 4, Article 1 of Decree No. 85/2021/ND-CP of the Government and Clause 6, Article 64 of Decree No. 98/2020/ND-CP of the Government. The former revised the scope of prohibited conduct concerning abusive multi-level marketing practices conducted through e-commerce activities, while the latter retained sanctioning language linked to an earlier formulation derived from Point (a), Clause 1, Article 4 of Decree No. 52/2013/ND-CP of the Government on E-commerce. This is not a minor drafting defect. It reveals a deeper structural problem in Vietnam's regulatory technique: prohibitions may be updated in one instrument while the corresponding sanctions remain tied to older wording in another. The consequence is weakened legal certainty, inconsistent interpretation by enforcement bodies, and greater room for procedural challenge by violators. In a regulatory environment that depends on administrative enforcement, such drafting misalignment directly reduces deterrent effect.

A third limitation lies in the institutional design of supervision and enforcement. Although the Personal Data Protection Law (2025) assigns supervisory functions to a specialized authority, the current model does not establish a fully independent supervisory body comparable to the data-protection authorities found in jurisdictions such as the European Union. The issue here is not simply institutional formality, but regulatory capacity and credibility. A supervisory mechanism embedded within a broader executive structure may face constraints in specialization, resource allocation, inter-agency coordination, and perceived impartiality, especially when violations involve powerful digital intermediaries or complex cross-border processing arrangements. In this respect, the legal framework remains more centralized than independent, and more administrative than truly regulatory in the specialized sense required by modern data governance.

A fourth weakness concerns the fragmentation of sanctioning competence. As indicated in Point (a), Clause 1, Article 4 and Clause 3, Article 52 of the Law on Handling of Administrative Violations (2012), read together with Clause 3, Article 6 of Decree No. 118/2021/ND-CP of the Government detailing the implementation of that Law, administrative enforcement should be governed by clear rules on jurisdiction and procedural authority. In practice, however, multiple authorities may potentially intervene in the same digital-market violation. This creates uncertainty not only over which body should act first, but also over which body should gather evidence, apply remedial measures, coordinate cross-sector information, and ensure procedural consistency. The underlying cause of this problem is institutional overlap without sufficiently precise jurisdictional demarcation. In traditional sectors, such overlap may be manageable. In digital markets—where violations can occur quickly, across jurisdictions, and through technically opaque systems—such ambiguity can delay intervention, dilute accountability, and undermine effective enforcement.

A fifth limitation concerns the law’s insufficient adaptation to the platform-based nature of modern data processing. The current framework still tends to regulate personal data through relatively linear legal categories—controller, processor, subject, sanctioning authority—whereas e-commerce ecosystems operate through layered, interdependent networks of data sharing, outsourcing, algorithmic profiling, and embedded third-party services. This mismatch between legal form and technological reality is one of the central reasons why enforcement remains difficult. The law is stronger at defining abstract rights

and obligations than at addressing the distributed, multi-actor character of actual data flows in platform commerce. As a result, legal responsibility can become diffused in practice, even where it appears clear in theory.

In addition to the new personal data protection regime, Vietnam has also adopted the Law on Artificial Intelligence (2025), which establishes a risk-based regulatory framework for AI systems. The law classifies AI systems into high-risk, medium-risk, and low-risk categories and introduces obligations relating to transparency, incident reporting, and human oversight. Importantly, the law explicitly requires that AI systems comply with regulations on personal data protection, cybersecurity, and intellectual property when collecting and processing data for training and operation. This regulatory linkage demonstrates the increasing convergence between data protection law and AI governance in Vietnam's digital regulatory architecture.

Taken together, these shortcomings indicate that the principal weakness of Vietnam's current legal framework is not the absence of regulation, but the incomplete conversion of legislative recognition into an integrated and enforceable governance system. The framework has become significantly more ambitious in normative terms, particularly following the adoption of the Personal Data Protection Law (2025) and related digital-governance legislation. These shortcomings also provide the analytical basis for the reforms proposed in the following section.

4.3 Recommendations and policy proposals

The weaknesses identified above suggest that the principal task for Vietnam is no longer to create a basic legal framework for personal data protection, but to transform existing legislative recognition into a coherent and enforceable governance system. The required reforms should therefore focus not only on expanding formal rights, but also on improving legal harmonization, procedural clarity, institutional specialization, and regulatory accountability.

First, the legal framework should be harmonized more systematically. One of the clearest weaknesses of the current regime lies in the coexistence of updated substantive rules and partially outdated sanctioning provisions. For this reason, Decree No. 98/2020/ND-CP of the Government should be comprehensively revised so that its

catalogue of violations, sanctions, and remedial measures is fully aligned with Decree No. 52/2013/ND-CP of the Government on E-commerce, as amended by Decree No. 85/2021/ND-CP, and with the Personal Data Protection Law (2025). Without such alignment, the legal system will continue to suffer from gaps between prohibited conduct and enforceable penalties, thereby weakening legal certainty and reducing deterrent effect.

Second, the statutory rights of data subjects should be made procedurally effective. Although Article 4 of the Personal Data Protection Law (2025) grants important rights, including access, withdrawal of consent, objection, restriction of processing, and deletion, those rights will remain only partially effective unless the law is supplemented by clearer implementation rules. In particular, the framework should specify how e-commerce platforms must verify requests, how quickly they must respond when data has already been shared with third parties, how compliance must be documented, and which party bears the evidentiary burden in the event of a dispute. In a platform-based environment, effective rights require operational procedures rather than abstract recognition alone.

Third, the law should better reflect the distributed nature of platform-based data processing. Current legal categories still assume relatively linear relationships between data subjects, controllers, and processors, whereas actual e-commerce ecosystems involve multiple interconnected actors. For this reason, clearer obligations should be imposed on platforms with respect to downstream data sharing, contractual responsibility, data-retention governance, and auditability across integrated service chains. E-commerce enterprises should also be required to adopt stronger internal compliance mechanisms, including transparent consent architecture, data-minimization practices, traceable data-sharing protocols, and technical safeguards capable of limiting secondary misuse.

Fourth, supervisory and enforcement capacity should be strengthened through greater institutional specialization. The present framework assigns supervisory functions to a specialized authority, but the current arrangement remains less independent and less specialized than the supervisory structures typically associated with mature data-protection regimes. Vietnam should therefore consider reinforcing the institutional autonomy, technical expertise, and inter-agency coordination capacity of the authority responsible for personal data protection. This is particularly important in cases involving

major digital intermediaries, complex cross-border processing, and technically sophisticated violations, where ordinary administrative enforcement may be too fragmented or too slow.

Fifth, jurisdictional fragmentation must be reduced. Where multiple agencies may intervene in the same digital-market violation, enforcement becomes slower, less predictable, and less accountable. Clearer jurisdictional rules are therefore needed to determine which authority should take the lead in investigating, sanctioning, coordinating evidence, and imposing remedial measures in cases involving consumer personal data in e-commerce. A more precise allocation of powers would improve procedural consistency and reduce institutional overlap.

Finally, public trust should be treated as a regulatory objective in its own right. Even the most detailed legal framework will remain incomplete if consumers do not understand how their data is processed, what risks they face, and what remedies are available when violations occur. Public guidance, compliance notices, more visible disclosure of enforcement actions, and targeted awareness campaigns would therefore complement legislative reform by making personal data governance more intelligible and more effective in practice.

Taken together, these reforms would help move Vietnam from a formally improved but still structurally incomplete legal framework toward a more integrated, enforceable, and credible model of personal data governance in the e-commerce sector.

5 CONCLUSION

Vietnam has made substantial progress in constructing a legal framework for the protection of consumers' personal data in e-commerce. The transition from a fragmented regime centered on personal information toward a more integrated statutory model reflects an important maturation of Vietnamese digital regulation.

Even so, legal development alone does not guarantee effective protection. Persistent weaknesses in normative coherence, supervisory design, sanctioning alignment, and the operationalization of data-subject rights continue to limit the practical effectiveness of the system. These weaknesses are especially evident in platform-based environments involving third-party sharing, technical opacity, and cross-border transfer.

For that reason, future reform should not focus solely on expanding formal rights, but also on improving enforceability, institutional coordination, and platform accountability. A more coherent and credible framework would better protect consumers, strengthen market trust, and support the long-term sustainability of Vietnam's digital economy.

REFERENCES

1. Civil Code of the Socialist Republic of Vietnam (2015).

2. Constitution of the Socialist Republic of Vietnam (2013).

3. De Hert, Paul; Papakonstantinou, Vagelis. The new General Data Protection Regulation: still a sound system for the protection of individuals? *Computer Law & Security Review*, v. 32, n. 2, p. 179–194, 2016.

4. Decree No. 13/2023/ND-CP on Personal Data Protection (2023).

5. Decree No. 52/2013/ND-CP on E-commerce (2013).

6. Decree No. 85/2021/ND-CP amending and supplementing a number of articles of Decree No. 52/2013/ND-CP on E-commerce (2021).

7. Decree No. 98/2020/ND-CP on administrative sanctions in commercial activities, the production and trading of counterfeit and prohibited goods, and the protection of consumer rights (2020).

8. Decree No. 118/2021/ND-CP detailing a number of provisions and implementation measures of the Law on Handling of Administrative Violations (2021).

9. E-Commerce and Digital Economy Agency. *Vietnam E-Commerce Report 2023*. Hanoi: Ministry of Industry and Trade, 2023. Available from: https://idea.gov.vn/?page=document. Access on: Jul. 15, 2025.

10. European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – GDPR). *Official Journal of the European Union*, L119, 4 May 2016.

11. General Department of Market Surveillance. Report No. 76/BC-TCQLTT dated Dec. 22, 2023 on the operational results of the Market Surveillance Force in 2023 and its tasks and orientations for 2024. Hanoi: Ministry of Industry and Trade, 2023.

12. General Department of Market Surveillance. Report No. 57/BC-TCQLTT dated Dec. 16, 2024 on the operational results of the Market Surveillance Force in 2024 and its tasks and orientations for 2025. Hanoi: Ministry of Industry and Trade, 2024.

13. Giang, Son. Strengthening the control of counterfeit and imitation goods on e-commerce platforms. *Thanh Tra Newspaper*, 2025. Available from: https://thanhtra.com.vn/an-ninh-trat-tu-D718A18CA/siet-kiem-duyet-hang-gia-hang-nhai-tren-san-thuong-mai-dien-tu-48a07c57c.html. Access on: Jul. 15, 2025.

14. Greenleaf, Graham. Global data privacy laws 2021: despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report*, n. 163, p. 10–13, 2021.

15. Kuner, Christopher. *Transborder Data Flows and Data Privacy Law*. 2nd ed. Oxford: Oxford University Press, 2017.

16. Kuner, Christopher; Bygrave, Lee; Docksey, Christopher (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford: Oxford University Press, 2020.

17. Law on Handling of Administrative Violations of the Socialist Republic of Vietnam (2012).

18. Law on Artificial Intelligence of the Socialist Republic of Vietnam (2025).

19. Law on Personal Data Protection of the Socialist Republic of Vietnam (2025).

20. Mayer-Schönberger, Viktor; Cukier, Kenneth. *Big Data: A Revolution That Will Transform How We Live, Work and Think*. London: John Murray, 2013.

Authors' Contribution

Data availability

All datasets relevant to this study's findings are fully available within the article.

How to cite this article (APA)

Nghia, L. T., & Tuan, N. M. (2026). GOVERNANCE OF CONSUMERS' PERSONAL DATA IN E-COMMERCE IN VIETNAM. *Veredas Do Direito*, 23, e235186. https://doi.org/10.18623/rvd.v23.5186