http://dx.doi.org/10.18623/rvd.v22.n2.3116

ENHANCING PERSONAL DATA PROTECTION ON E-COMMERCE PLATFORMS: A CASE STUDY IN VIETNAM

MELHORAR A PROTEÇÃO DE DADOS PESSOAIS EM PLATAFORMAS DE COMÉRCIO ELETRÔNICO: UM ESTUDO DE CASO NO VIETNÃ

Article received on: 6/23/2025
Article accepted on: 9/29/2025

Nguyen Le Minh*
* Ho Chi Minh City University of Law
Vietnam
Orcid: https://orcid.org/0009-0006-2244-048X
leminhcantho@gmail.com

Ha, Thi Thanh Binh*
* Ho Chi Minh City University of Law
Vietnam
Orcid: https://orcid.org/0009-0005-2029-2033
httbinh@hcmulaw.edu.vn

The authors declare that there is no conflict of interest

Abstract
In the context of Vietnam's rapidly expanding e-commerce market, personal data has become a critical asset, driving personalization, marketing optimization, and strategic decision-making. However, its use raises significant concerns about consumer privacy. This paper examines the methods of personal data collection and utilization in e-commerce activities, categorizing them into user-provided data (sign-up forms, surveys, reviews) and automatically collected data (cookies, NLP, web scraping). The research examines the diverse roles of data in improving customer experience, streamlining logistics, optimizing customer service, and preventing fraud. A key aspect is the examination of Vietnam's legal framework concerning personal data protection, especially following the milestone enactment of Decree No. 13/2023/ND-CP and Law No. 91/2025/QH15 on Personal Data Protection. While these legislative developments mark a considerable stride towards aligning with international norms, the study highlights notable implementation obstacles. Such obstacles encompass low public understanding, the lack of an autonomous Data Protection Authority (DPA), vagueness in legal definitions, and compliance complexities faced by small and medium-sized enterprises (SMEs). Based on this analysis, the paper proposes specific policy recommendations to bridge the gap between legislation and practice, including the establishment of an independent DPA, the issuance of detailed guidelines, enhanced support

Resumo
No contexto do mercado de comércio eletrônico em rápida expansão do Vietnã, os dados pessoais tornaram-se um ativo crítico, impulsionando a personalização, a otimização de marketing e a tomada de decisões estratégicas. No entanto, seu uso levanta preocupações significativas sobre a privacidade do consumidor. Este artigo examina os métodos de coleta e utilização de dados pessoais em atividades de comércio eletrônico, categorizando-os em dados fornecidos pelo usuário (formulários de inscrição, pesquisas, avaliações) e dados coletados automaticamente (cookies, PLN, web scraping). A pesquisa examina os diversos papéis dos dados na melhoria da experiência do cliente, na simplificação da logística, na otimização do atendimento ao cliente e na prevenção de fraudes. Um aspecto fundamental é a análise do arcabouço legal do Vietnã relativo à proteção de dados pessoais, especialmente após a promulgação histórica do Decreto nº 13/2023/ND-CP e da Lei nº 91/2025/QH15 sobre Proteção de Dados Pessoais. Embora esses desenvolvimentos legislativos marquem um avanço considerável em direção ao alinhamento com as normas internacionais, o estudo destaca obstáculos notáveis à implementação. Tais obstáculos incluem a baixa compreensão pública, a ausência de uma Autoridade de Proteção de Dados (APD) autônoma, a imprecisão nas definições legais e as complexidades de conformidade enfrentadas por pequenas e médias empresas (PMEs). Com base

for SMEs, and the promotion of public education programs to raise community awareness.

Keywords: Personal Data. E-commerce. Vietnam. GDPR. Consumer Trust.

nessa análise, o artigo propõe recomendações políticas específicas para preencher a lacuna entre a legislação e a prática, incluindo o estabelecimento de uma APD independente, a emissão de diretrizes detalhadas, o reforço do apoio às PMEs e a promoção de programas de educação pública para conscientizar a comunidade.

Palavras-chave: *Dados Pessoais. Comércio Eletrônico. Vietnã. GDPR. Confiança do Consumidor.*

1 INTRODUCTION

The explosive growth of e-commerce has revolutionized how businesses operate and consumers interact with marketplaces, ushering in a data-driven economy where personal data has become a crucial asset. E-commerce platforms, in particular, are heavily reliant on the collection, analysis, and utilization of consumer data to enhance user experiences, personalize services, optimize operations, and generate targeted advertising revenue. However, this increasing dependence has also brought forth profound concerns regarding data privacy, security, and related ethical issues.

In the global context, regulatory frameworks such as the European Union's General Data Protection Regulation (GDPR) have established stringent standards for the collection and processing of personal data. These regulations emphasize core principles such as the explicit consent of data subjects, transparency, data minimization, and accountability, compelling organizations worldwide to reconsider their data protection strategies. The GDPR's influence has extended beyond Europe, prompting Asian jurisdictions, including Vietnam, to strengthen their domestic data protection regulations.

Vietnam's digital economy has experienced remarkable growth, with e-commerce emerging as a cornerstone of this transformation. Recognizing personal data as a strategic national asset, the Government introduced Decree No. 13/2023/ND-CP on Personal Data Protection a pivotal legal instrument designed to align Vietnam's data governance model with international best practices. This decree marks a significant shift from a previously fragmented regulatory landscape toward a more coherent and rights-based approach to data protection. The ongoing evolution of this framework, including the forthcoming Law No. 91/2025/QH15, aims to further solidify these protections. However, despite these advancements and a general focus on the multifaceted role of data in customer experience,

logistics, customer service, and fraud prevention, the implementation faces substantial challenges. These include low public awareness, the absence of an independent Data Protection Authority (DPA), ambiguity in legal terminology, and compliance difficulties for small and medium-sized enterprises (SMEs).

Despite these regulatory advancements, the practical implementation of personal data protection measures within Vietnam's e-commerce sector continues to face significant challenges. Many small and medium-sized enterprises (SMEs) struggle with compliance due to limited resources, while consumer awareness of their data rights remains relatively low. Furthermore, regulatory ambiguities and the absence of a dedicated independent supervisory authority can weaken enforcement effectiveness and erode user trust.

This study aims to address these gaps by examining the comprehensive legal and operational landscape of personal data protection on Vietnamese e-commerce platforms. Through an in-depth literature review and a strategic SWOT analysis, the research aims to: (i) evaluate the strengths and limitations of the current legal framework, (ii) assess the implementation status across various e-commerce entities, and (iii) propose actionable solutions for improving data protection practices. The research findings are expected to provide valuable insights for policymakers, platform operators, and consumers alike, contributing to navigation within Vietnam's continually evolving data privacy legal environment.

2 LITERATURE REVIEW

The critical role of e-commerce platforms in personal data protection is amplified within rapidly growing digital economies like Vietnam. As online transactions proliferate globally and locally, the intersection of data privacy, technological advancement, and consumer trust has become a central concern for researchers, practitioners, and policymakers alike. Ensuring a responsible data ecosystem is paramount for the sustainable growth of e-commerce.

Internationally, regulations like the GDPR have established significant benchmarks for how organizations, including e-commerce platforms, must handle personal data. The GDPR framework particularly addresses complex issues such as the use of artificial intelligence (AI) in processing personal data and profiling consumers

(European Parliament, Directorate General for Parliamentary Research Services, 2020), setting a high standard for compliance and ethical data management. While GDPR provides an influential global backdrop, the specific regulatory landscape within individual jurisdictions is crucial. In Vietnam, personal data is understood as information in the form of symbols, letters, numbers, images, sounds, or similar formats in electronic environments that are associated with or help identify a specific individual (thuvienphapluat.vn, n.d.). Personal data includes both basic personal data and sensitive personal data. Thus, personal data refers to individual information that helps identify a specific person, which is formed from that individual's activities and, when combined with other stored data and information, enables identification. Vietnamese law clearly outlines specific obligations for personal data controllers and processors, including domestic e-commerce platforms. However, understanding the practical challenges in implementing and enforcing these new regulations in the Vietnamese context remains an area that requires further exploration. Consumer trust is intrinsically linked to effective data protection. Research consistently indicates that consumers are highly sensitive to how their personal data is handled, and privacy concerns can directly impact their purchasing behavior and loyalty towards e-commerce platforms (Schäfer *et al*., 2023). This sensitivity underscores the responsibility of companies to prioritize data protection, as breaches or perceived misuse of data can lead to significant reputational damage and erosion of customer trust.

In a study on user attitudes in Vietnam, James Cho and Colleagues pointed out that information quality, perceived security, perceived privacy, and consumer trust influence the intention to shop online in Vietnam. The results show that perceived privacy and consumer trust have a positive and significant impact on online shopping intention. This highlights the importance of protecting personal data and building trust in the Vietnamese e-commerce environment (Cho *et al*., 2023). While this general consumer attitude is well-documented, specific insights into the awareness levels, primary concerns, and expectations of Vietnamese consumers regarding data privacy in their online shopping experiences are vital for platforms operating locally.

Navigating the complexities of the digital environment requires e-commerce platforms to develop robust and multifaceted data strategies. Achieving a delicate balance between leveraging data for personalization and business growth and the imperative to protect consumer privacy necessitates not only compliance with legal standards but also

the proactive implementation of technical and organizational measures(Quach *et al*., 2022). Effective privacy protections, such as the integration of secure payment gateways, end-to-end data encryption, and robust authentication mechanisms, are essential technical safeguards that underpin secure digital transactions and foster consumer confidence (Morić *et al*., 2024). Beyond technical solutions and legal compliance, the ethical dimension of data privacy is critical. An ethical approach to data management involves embedding principles of transparency, fairness, and data minimization into business practices, prioritizing consumer rights and data security (Lee *et al*., n.d.). E-commerce platforms must consciously consider the broader societal implications of their data practices, ensuring alignment with ethical norms to maintain long-term trust and social license to operate.

In summary, the literature establishes the global significance of robust legal frameworks (like GDPR and now Vietnam's Decree 13 or Law No. 91/2025/QH15), the paramount importance of consumer trust influenced by privacy perceptions, and the need for e-commerce platforms to implement comprehensive technical and ethical data protection strategies. However, while these general principles are clear, there is a discernible gap in empirical research examining the specific ways in which e-commerce platforms operating within the unique Vietnamese market are currently adapting to and implementing these data protection measures, particularly in light of the recent Decree 13/2023/NĐ-CP. Limited research exists on the practical challenges faced by these platforms in Vietnam, the effectiveness of their adopted strategies, and how these strategies are perceived by Vietnamese consumers. Therefore, this study, utilizing a case study approach focused on Vietnam, aims to address this gap. It seeks to provide an in-depth understanding of the current practices, challenges, and potential enhancements for personal data protection on e-commerce platforms within the Vietnamese context, offering valuable insights for platforms, policymakers, and users in this dynamic digital landscape.

3 DATA SET AND METHODS

This study employs a qualitative research methodology to explore the current state and regulatory challenges of personal data protection in Vietnam's e-commerce sector. The dataset consists of secondary sources, including government regulations (notably

Decree No. 13/2023/NĐ-CP), policy documents, academic literature, and publicly available reports and survey data from relevant institutions such as the Ministry of Industry and Trade, Statista, and DataReportal. These sources provide a comprehensive foundation for understanding the intersection of legal frameworks, platform practices, and consumer perspectives.

To analyze the qualitative data, the study adopts a thematic analysis approach. This method allows for the systematic identification, organization, and interpretation of key patterns (themes) within the data. Thematic analysis was chosen because it offers flexibility and depth in examining how data protection is framed legally, implemented operationally, and perceived socially across different stakeholder groups. The process followed Braun and Clarke's (2006) six-phase model: (1) familiarization with the data through iterative reading; (2) generating initial codes based on recurring concepts related to data protection and compliance; (3) searching for themes such as "consumer trust," "regulatory enforcement," and "SME challenges"; (4) reviewing themes for internal coherence and relevance to the research questions; (5) defining and naming themes; and (6) producing the analytical narrative grounded in examples and excerpts from the materials reviewed. This qualitative analysis is complemented by a SWOT (Strengths, Weaknesses, Opportunities, Threats) framework, which provides a structured lens for evaluating the regulatory environment and identifying strategic pathways for improvement. The triangulation of thematic analysis with the SWOT framework strengthens the reliability and analytical rigor of the research. While the study primarily relies on secondary data, the integration of diverse sources and a transparent analytical method ensures that the findings are robust, context-sensitive, and policy-relevant. Future research could further enhance this analysis through primary data collection, such as interviews with platform operators, policymakers, and consumers.

4 FINDINGS AND DISCUSSIONS

4.1 Methods of personal data collection and utilization in e-commerce

4.1.1 Methods of personal data collection in e-commerce activities

In the digital age, personal data has become an invaluable asset for e-commerce platforms aiming to better understand their customers and enhance the shopping experience. To maintain a competitive edge, businesses must continuously collect, analyze, and leverage user data to personalize services, predict behavior, and improve engagement. Various methods are used to gather this data, each offering distinct insights and serving specific purposes. This analysis explores six common personal data collection methods employed by e-commerce platforms, categorized into two main groups: user-provided data and automatically collected data.

Figure 1.

Methods for collecting e-Commerce data

Sign-Up Forms: Sign up forms serve as the initial and most critical interaction point on e-commerce sites, where users voluntarily submit personal information such as names, email addresses, phone numbers, and occasionally product preferences in order to create accounts, place orders, or join marketing communications (softcircles, n.d.). This willingly provided data is indispensable for account management, order tracking, and maintaining contact lists for email or SMS marketing, making sign-up forms both effective and transparent . However, research consistently shows that long or intrusive

forms significantly hinder conversions even a single extra field averted contributed to Expedia losing over $12 million annually and simpler forms with fewer required fields dramatically boost sign-up rates.

Surveys: Surveys are a powerful research tool for gathering detailed user information, as they allow e-commerce platforms to ask customers targeted questions about demographics, purchasing behaviors, satisfaction levels, and expectations (Yong *et al*., 2023). Often deployed post-purchase or within broader market research campaigns, surveys can uncover nuanced insights into user experiences and preferences. However, the accuracy and usefulness of survey data heavily depend on respondents' willingness to take part and the honesty of their answers. Self-report data are known to be affected by factors such as response bias, including social desirability or acquiescence which can distort findings and limit their reliability.

Customer Reviews: Customer reviews serve as a critical feedback channel, allowing businesses to gather insights for service improvement. However, the value of these reviews extends beyond data collection to the practice of online reputation management. A key aspect of this involves a firm's active engagement with customer feedback. Research by Proserpio and Zervas (2017) provides empirical evidence that management responses to reviews can significantly improve a brand's reputation. Specifically, their study found that businesses that actively respond not only receive more reviews but also tend to achieve higher ratings in the future. This action signals that the business is attentive and values its customers, thereby strengthening consumer trust. In turn, this enhanced trust, reflected in an improved reputation, can indirectly support higher conversion rates and foster long-term customer loyalty (Proserpio and Zervas, 2017).

Cookie Tracking: Cookies are small data files stored on a user's browser when visiting a website, enabling the tracking of behaviors such as visited pages, clicks, and session durations. This tracking underpins key functions in e-commerce such as personalizing product suggestions, serving targeted advertisements, and optimizing user interfaces. However, as Nouwens *et al*. (2025) emphasize, the ecosystem of online tracking remains legally and ethically contentious. Despite regulations like the GDPR and the ePrivacy Directive, only 15% of cookie consent interfaces are minimally compliant, often lacking meaningful reject options or offering interfaces skewed toward acceptance. The authors argue that cookie banners, while superficially complying with consent laws,

frequently obscure the true extent and nature of tracking, raising concerns about transparency and user autonomy (Nouwens *et al*., 2025).

Natural Language Processing (NLP): NLP is a branch of artificial intelligence (AI) that can process and interpret human language. In e-commerce, NLP is applied to analyze unstructured text sources like customer feedback, reviews, chat messages, and search queries. This technology helps businesses capture customer sentiment, preferences, and potential issues. By transforming text into actionable insights, NLP directly contributes to strategic decision-making and service improvements.

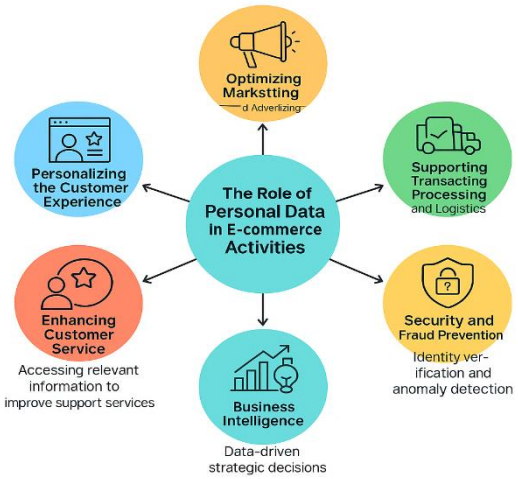
Web Scraping: Web scraping is a technique for automatically extracting data from external websites, including competitor sites, price comparison portals, and public directories. E-commerce platforms use this method to gather market intelligence, track competitors' pricing strategies, or monitor product availability. While it provides a panoramic view of the market landscape, web scraping can raise ethical and legal issues, especially when it violates a site's terms of service.

The six methods discussed above, from sign-up forms, surveys, and customer reviews to cookie tracking, NLP, and web scraping, form a comprehensive toolkit for e-commerce platforms to collect and leverage personal data. A skillful combination of user-provided and automatically collected data allows businesses to build a 360-degree view of their customers. However, in a context where users are increasingly concerned about privacy, data collection must be accompanied by transparency and compliance with legal regulations, ensuring a balance between the goal of personalizing experiences and respecting consumer rights.

The Role of Personal Data in E-commerce Activities: Personal data plays an increasingly vital role across all aspects of e-commerce operations. It enables businesses to personalize user experiences, optimize marketing efforts, streamline transactions and logistics, improve customer service, and enhance both strategic planning and fraud prevention. These applications not only improve operational efficiency but also contribute to building trust and long-term customer relationships. The diverse roles of personal data in e-commerce are summarized in **Figure 2.**

Figure 2.

Roles of Personal Data in E-commerce



Source: Created by the authors.

Personalizing the Customer Experience: Personal data plays a pivotal role in personalizing and enhancing the customer experience on e-commerce platforms by crafting a unique and tailored shopping journey for each user. Algorithmic and machine learning systems process user data to track and analyze their behavior and preferences. For instance, prominent platforms like Amazon, Shopee, and Tiki leverage browsing history (via cookies), purchase history, items added to the cart or wish list, and even the duration a user views a particular product to generate features such as "Recommended for you" or "Similar products." A user who frequently searches for and purchases books on economics will likely see related book suggestions, targeted advertisements, or promotional emails for online courses in the same domain. This approach not only aims to suggest relevant products, customize the user interface, and deliver targeted marketing messages, but also helps businesses anticipate individual needs, thereby enhancing customer satisfaction and significantly improving purchase conversion rates. Indeed, businesses adept at personalization are reported to achieve up to a 40% revenue increase from such activities compared to their counterparts (Hassan *et al*., 2025).

In Vietnam's intensely competitive digital retail landscape, such personalized experiences have transitioned from a differentiator to a standard expectation. The efficacy of recommendation engines is intrinsically linked to the quality and quantity of available user data, compelling platforms to actively amass granular-level information to refine their algorithmic capabilities. This imperative, however, concurrently raises salient

concerns regarding the ethical boundaries of data utilization and the substantive adequacy of user consent mechanisms.

Optimizing Marketing and Advertising Strategies with Personal Data: Personal data serves as a foundational element in developing effective digital marketing and advertising campaigns. Instead of relying on mass advertising, businesses can utilize this data to segment and precisely target potential customer groups, thereby optimizing budgets and increasing conversion rates. For example, a fashion brand promoting its new summer collection can leverage demographic data (age, gender, geographic location) combined with interest-based data (collected from social media interactions, past shopping behavior) to run ads on platforms like Facebook or Instagram, for instance, targeting beach dresses to women aged 18-35 living in coastal cities with an interest in travel. Furthermore, tracking pixels on websites enable retargeting individuals who viewed products but did not make a purchase. This is part of sophisticated digital advertising and monetization strategies where user profiling and behavioral targeting allow e-commerce platforms and third-party advertisers to deliver advertisements based on users' online activities, stated preferences, and purchase history. According to the Vietnam Digital Advertising Market report ("Digital in Vietnam," n.d.), over 60% of ad impressions on e-commerce platforms were behaviorally targeted, a practice underpinned by real-time data analytics and programmatic advertising frameworks. Key data sources for these strategies include demographic profiles, online interests, ad interaction history, tracking pixel data, and shopping behaviors such as purchase frequency and average order value.

Supporting Transaction Processing and Logistics: Accurate personal information is fundamental for the seamless execution of the entire e-commerce order fulfillment process, from initial placement and payment processing to final delivery. The precision of this data directly contributes to minimizing errors, which in turn reduces potential operational inefficiencies, additional costs, and safeguards brand reputation (Groenewald, 2024). For instance, when completing a purchase on platforms like Tiki or Lazada, customers are required to provide their full name, a verifiable delivery address, a contact phone number, and an email address. This data, typically collected through registration or order forms, is not merely administrative; it is operationally critical. It is used to confirm orders, disseminate real-time status updates, and, most importantly, enable third-party logistics (3PL) providers such as Giao Hang Nhanh or J&T Express to successfully

deliver products to the correct recipient. The critical role of data accuracy in last-mile delivery success and its impact on customer satisfaction has been widely documented (Raj *et al*., 2024). Indeed, even minor inaccuracies in the provided address or phone number can lead to significant disruptions, such as failed deliveries, increased return rates, and frustrated customers (Viu-Roig and Alvarez-Palau, 2020). Therefore, the integrity of customer-provided information during account registration or order placement, including name, address, phone number, and email, along with transaction history, forms the bedrock of an efficient e-commerce logistics network.

Enhancing Customer Service through Personal Data Analysis and Utilization: Personal data plays a pivotal role in transforming and enhancing both the efficiency and quality of customer support services in the e-commerce environment. By enabling support staff to access relevant customer information, businesses can equip their teams with a deep understanding of the context and history of each specific case, thereby providing faster, more accurate, and highly personalized solutions (Sulastri, 2023). This not only resolves issues effectively but also significantly improves the overall customer experience, contributing to building loyalty. For instance, when a customer contacts the support center of a telecom provider like Viettel or FPT Telecom to report a service issue, the customer service representative can instantly retrieve data from the Customer Relationship Management (CRM) system. This system stores records of previous calls, current service plans, payment history, and notes from past interactions. With this information, the agent can avoid asking repetitive questions and instead directly address the customer's issue efficiently and empathetically, an approach proven to increase customer satisfaction (Kumar *et al*., 2022). Key data sources underpinning this capability include service usage and purchase history, communication records (emails, chats, calls), account information, and notes from previous support agent interactions.

Decision Making through Aggregated Data Analysis and Business Intelligence: Aggregated data, often anonymized or analyzed at a macro level, provides deep insights into market dynamics, consumer trends, and operational performance, thereby empowering businesses to make evidence-based strategic decisions. This process is at the core of Business Intelligence (BI), which helps transform raw data into actionable insights (Choi *et al*., 2018). For instance, an online retail chain like Thegioididong can analyze sales data by region, product category, and period using its sales management systems and transaction data. If the analysis reveals a surge in iPhone sales in Ho Chi Minh City

following a product launch, while customers in Hanoi show a stronger preference for Samsung devices, the company can adjust its inventory planning, marketing campaigns, and resource allocation appropriately and promptly. Beyond sales data, customer feedback and product reviews collected via website rating sections and post-purchase surveys also provide invaluable input for product development and service improvement. Effectively leveraging these diverse data sources to create a competitive advantage and guide development is a testament to the successful application of BI (Ahmad, 2015). Key data sources for such Business Intelligence initiatives include transaction data (sales volume and value), website analytics (traffic, bounce rate), customer feedback, survey results, and marketing campaign data.

Enhancing Security and Fraud Prevention in E-commerce through Personal and Behavioral Data: Personal data, particularly user behavioral patterns, plays a central role in verifying user identities and detecting suspicious activities on e-commerce platforms, thereby safeguarding assets for both customers and businesses. Modern fraud prevention systems rely not only on static information but also dynamically analyze user interactions (Zhang *et al*., 2025). For example, online payment gateways like VNPay or commercial banks handling e-commerce transactions often deploy sophisticated algorithms. These algorithms analyze users' transaction histories, login IP addresses, and device information (device fingerprinting), comparing them against pre-identified fraud patterns. If a user account that typically processes transactions within Vietnam suddenly initiates a large transaction from a foreign IP address using an unfamiliar device, the system may identify this as anomalous behavior and trigger protective measures. In such cases, the transaction may be temporarily blocked and require additional verification, such as an OTP (One-Time Password) sent to the registered phone number, to prevent potential fraud. This behavior-based anomaly detection mechanism is a critical line of defense, helping to mitigate financial risks and maintain user trust in the system. Key data sources for these systems include login credentials, IP addresses, transaction history, device metadata, login behavior (time, location, frequency), and biometric data when available.

4.2 Legal framework and compliance challenges in Vietnam

Legal Regulations on Personal Data Protection in Vietnamese E-commerce: The legal framework surrounding personal data protection in Vietnam has evolved

significantly over the past decade, particularly in response to the rapid digitalization of commerce and the increasing volume of data being collected and processed online. As Vietnam positions itself as a digital economy leader in Southeast Asia, the need for comprehensive, enforceable, and forward-looking data protection laws has become increasingly urgent. This section explores the development of Vietnam's legal instruments related to personal data protection, evaluates the strengths and limitations of the current framework, especially in the context of e-commerce platforms, and considers implementation challenges on the ground.

Historically, the Vietnamese legal framework governing personal data protection was characterized by a fragmented approach, lacking a singular, comprehensive statute. Instead, provisions about data were dispersed across various legislative instruments. These included the Law on Cyber Information Security (2015), which established foundational principles for data processing and the necessity of user consent; the Law on Cybersecurity (2018), which introduced more stringent obligations regarding data localization and delineated platform responsibilities in the context of national security and both the Civil Code (2015) and the Law on Protection of Consumer Rights (2023), which acknowledged, in principle, individuals' rights to the protection of their personal information.

While this amalgamation of laws provided a rudimentary foundation, it failed to furnish a unified legal definition of "personal data," nor did it clearly delineate the specific rights of data subjects or the correlative responsibilities incumbent upon data controllers and processors. This pre-existing regulatory lacuna consequently engendered legal uncertainty, leaving many data processing practices prevalent on e-commerce platforms either unregulated or subject to ambiguous governance (Nguyen *et al*., 2024).

The promulgation of Decree No. 13/2023/NĐ-CP marks a milestone in Vietnam's legal framework on data privacy. It is the country's first comprehensive legal instrument dedicated to personal data protection and demonstrates strong alignment with leading international standards, such as the GDPR. With this decree, Vietnam establishes a unified regulatory framework governing the collection, processing, storage, transfer, and protection of personal data across all sectors.

Key provisions include: (i) Clear Definitions of Personal Data: The Decree distinguishes between basic personal data (e.g., name, phone number) and sensitive personal data (e.g., biometric data, financial information, location data), with heightened

protection for the latter. (ii) Consent-Based Processing: All data processing activities must be based on the voluntary, explicit, and informed consent of the data subject, except in legally defined exemptions. (iii) Obligations for Data Controllers and Processors: E-commerce platforms must implement technical and organizational measures to ensure data security, maintain internal records of processing activities, and appoint personnel responsible for data protection. (iv) Rights of Data Subjects: Users are entitled to access, correct, delete their data, and withdraw consent at any time. (v) Cross-Border Data Transfer Restrictions: Personal data transfers outside Vietnam are subject to government approval and must meet data sovereignty requirements.

From a legal perspective, the decree signifies a move toward a rights-based data governance model. However, unlike comprehensive data protection laws in other jurisdictions, Decree 13 is not a National Assembly-passed law, but an administrative instrument issued by the Government, which may limit its enforceability and long-term stability.

The Current State of Personal Data Protection on Vietnamese E-commerce Platforms*:* E-commerce platforms operating within Vietnam, encompassing both domestic and international entities, are unequivocally bound by the obligations stipulated in Decree No. 13/2023/NĐ-CP. These legal mandates necessitate, inter alia, the establishment of transparent privacy policies, the implementation of robust mechanisms for obtaining and managing user consent, the maintenance of secure data storage infrastructure (preferably localized within Vietnam in alignment with cybersecurity regulations), and the development of comprehensive data breach response protocols. Notwithstanding these clear legal requirements, the practical implementation across the e-commerce landscape exhibits considerable heterogeneity. While prominent platforms such as Shopee, Lazada, and Tiki have demonstrably undertaken measures to revise their privacy policies and invest in dedicated data protection officers and internal compliance teams, a significant proportion of smaller platforms and third-party sellers often contend with resource constraints or a deficit in awareness, thereby impeding their capacity to fully adhere to the Decree's provisions. Illustrative of this disparity, a 2023 survey conducted by the Vietnam Digital Economy Group (VDEG) revealed that a mere 38% of local e-commerce small and medium-sized enterprises (SMEs) possessed formal data governance frameworks, with a concerning 62% reportedly unaware of the comprehensive implications and requirements imposed by Decree 13 (Trade, n.d.). This

highlights a critical gap between regulatory intent and on-the-ground compliance within the sector.

Vietnam's approach to data protection is increasingly influenced by global trends and trade agreements. The CPTPP and EVFTA trade agreements contain clauses on data protection and cross-border data flows, requiring Vietnam to strike a balance between national sovereignty and global interoperability. Decree 13 signals a willingness to align with international norms, but practical alignment with the GDPR or APEC Privacy Framework remains a work in progress.

Scholars have also noted that Vietnam's regulatory model reflects a state-centric approach, prioritizing national security and social order over individual data rights. This can sometimes lead to tension between privacy protection and government surveillance imperatives, particularly in the name of cybersecurity.

Despite the regulatory advances, several challenges persist in turning legal provisions into effective practice:

Low Public Awareness and Education: Without strong digital literacy among users, the rights granted under the law (such as data access and deletion) remain largely underutilized. This hinders user empowerment, a critical goal of any data protection regime. Within the contemporary digital economy, personal data has emerged as an asset of paramount commercial significance, particularly within the e-commerce sector. The increasing migration of consumer transactions to online environments endows e-commerce platforms with a substantial competitive advantage derived from their capacity to collect, analyze, and strategically leverage such data. In the Vietnamese context, where the e-commerce market exhibits consistent double-digit annual growth ("eCommerce - Vietnam | Statista Market Forecast," n.d.), personal data assumes a critical function in the personalization of services, the cultivation of customer relationships, and the formulation of strategic business decisions.

This monetization of personal data implicates significant issues concerning informed consent and the commodification of individual information. A considerable segment of users in Vietnam remains unaware of the extent to which their data is processed beyond the immediate transactional context. A study conducted by Nguyen *et al* revealed that 58% of Vietnamese online shoppers were oblivious to their behavioral data being disseminated to third-party entities (NGUYEN and CHUNG, 2022). Such informational and power asymmetry between platforms and consumers epitomizes the

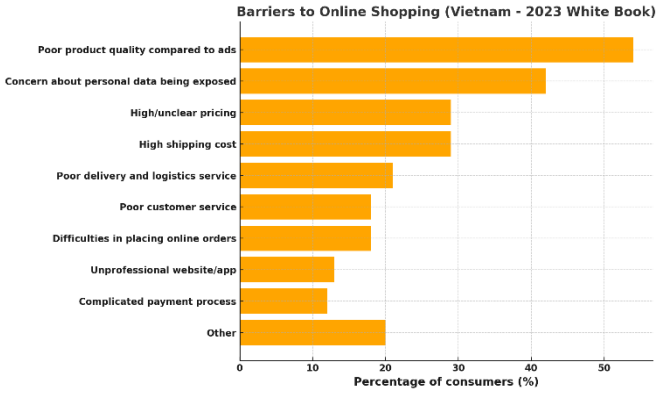
"data privacy paradox" (Norberg *et al*., 2007), wherein individuals continue to disclose data despite professed privacy concerns, often due to a perceived lack of viable alternatives or a deficit in comprehension.

Pursuant to Decree No. 13/2023/NĐ-CP, personal data in the Vietnamese jurisdiction encompasses any information that identifies, or is capable of being associated with the identity of, a natural person. This includes data that directly (e.g., name, identification number) or indirectly (e.g., location data, transaction history, behavioral preferences) pertains to an individual. Within the operational ambit of e-commerce platforms, such data typically comprises customer profiles, contact particulars, delivery addresses, purchase histories, payment modalities, browsing behaviors, device identifiers, and interaction logs with the platform's website or application.

The study reveals that a significant portion of Vietnamese consumers express notable concerns regarding the collection and use of their personal data by e-commerce platforms ("White Book of Viet Nam Information and Communication Technology 2023," n.d.) **(Figure 3)**.

Figure 3.

Vietnam – 2023 White Book



Source: Ministry of Science and Technology

While users increasingly engage in online transactions and exhibit improved digital literacy, there remains a substantial gap in their understanding of what constitutes personal data and how it is legally protected under Vietnamese regulations, such as Decree No. 13/2023/NĐ-CP. The study found that stringent data privacy regulations positively influence consumer trust in e-commerce platforms. When consumers perceive that their data is adequately protected, they are more likely to trust the platform, resulting

in higher confidence levels and increased willingness to engage in online transactions (Jack Trọng, 2024).

Lack of Clear Enforcement Authority: There is currently no independent data protection authority in Vietnam akin to the EU's DPAs. Instead, oversight is divided among various ministries (e.g., the Ministry of Public Security, the Ministry of Information and Communications), which can result in regulatory overlap or fragmentation.

Ambiguity in Legal Terminology: Concepts such as "informed consent," "legitimate interest," or "sensitive data processing" remain vaguely defined, creating compliance uncertainty for businesses.

Resource Constraints for SMEs: Smaller firms often cannot afford data protection officers or legal experts, creating a compliance gap that may undermine the overall effectiveness of the law.

Cross-border Enforcement Complexity: Vietnam's ability to regulate international e-commerce giants is limited, especially in enforcing consent and data processing requirements on foreign-hosted websites.

4.3 Policy recommendations for addressing development gaps in Vietnam

In light of the evolving digital landscape and the pressing need to strengthen personal data governance, Vietnam faces a critical juncture in its regulatory development. While recent legislative advancements mark important progress, persistent gaps remain in terms of enforcement mechanisms, institutional coherence, practical guidance, and stakeholder engagement especially for vulnerable sectors such as small and medium-sized enterprises (SMEs) and individual data subjects. To bridge these gaps and align Vietnam's personal data protection framework with international best practices, this section proposes a set of strategic and actionable policy recommendations. These recommendations draw from established global models, academic research, and regional experiences, and are tailored to the Vietnamese context to ensure both effectiveness and feasibility. They include the establishment of an independent Data Protection Authority (DPA), the issuance of clear legal guidance, enhanced support for SMEs, public education initiatives, and the promotion of international cooperation and extraterritorial enforcement.

Proposal for the Establishment of an Independent Data Protection Authority (DPA) in Vietnam: It is hereby proposed that an Independent DPA be established in Vietnam. This authority shall be constituted as a specialized, independent body, vested with the requisite authority, resources, and expertise to effectively oversee and enforce personal data protection legislation. The DPA shall function as the sole and central competent authority responsible for all matters pertaining to personal data. Its mandate shall encompass investigative powers, the imposition of sanctions for infringements, the issuance of detailed guidance, and the implementation of public awareness initiatives.

The viability and efficacy of this proposal are substantiated by reputable international frameworks, academic discourse, and regional experiences:

The GDPR: Articles 51-59 of the GDPR explicitly mandate the establishment and delineate the roles of Supervisory Authorities (DPAs) within each Member State. The operational models of effective DPAs, such as the Information Commissioner's Office (ICO) in the United Kingdom and the Commission Nationale de l'Informatique et des Libertés (CNIL) in France, serve as pertinent exemplars.

The critical function of DPAs is well recognized in the scholarly literature. Aaron Ceross, for instance, identifies DPAs, exemplified by the UK's ICO, as central to supervising, investigating, penalizing, and guiding organizations in the protection of personal data. Ceross underscores the principle that privacy rights are not self-enforcing, thereby necessitating a specialized body endowed with comprehensive, lawful, and independent enforcement mechanisms (Ceross, 2018). Concurring with this perspective, Yulia Neta *et al*. posit that DPAs play a crucial role in overseeing compliance with personal data protection laws across both public and private sectors (Neta *et al*., 2022).

Furthermore, international experience within the Asian region, notably in Singapore with its Personal Data Protection Commission (PDPC) and the Philippines with its National Privacy Commission (NPC), demonstrates the successful establishment and positive outcomes of DPAs in safeguarding personal data, thereby affirming the model's applicability and efficacy within a comparable regional context.

The establishment of such a DPA is anticipated to ensure consistency and a high degree of specialization in data protection endeavors, mitigate functional overlaps among existing state agencies, and thereby substantially enhance the effectiveness of legislative enforcement. Crucially, the presence of a demonstrably independent and competent DPA

will serve to bolster public and business confidence in the national personal data protection regime.

Issuing Detailed Guidelines and Clear Definitions: The competent authority ideally, the newly established Data Protection Authority (DPA) should issue secondary legislation, such as decrees, circulars, and official guidelines to clarify key legal terms under personal data protection laws. These definitions must be specific, easy to understand, and should include illustrative examples to support practical application.

Examples include: (i) “Informed consent”: Consent must be voluntary, specific, and based on complete information (including purpose of processing, scope, duration, third-party sharing, etc.), and must be easily revocable. (ii) “Legitimate interest”: Guidance should include the commonly adopted "three-part test" used by many DPAs globally: (1) identify the legitimate interest; (2) assess the necessity of processing to achieve that interest; and (3) balance it against the rights and interests of the data subject. (iii) “Sensitive data processing”: The authority should list the types of data considered sensitive and require stricter protection measures for such data.

The EU’s General Data Protection Regulation (GDPR), particularly Article 4, provides comprehensive definitions of key terms (“Art. 4 GDPR – Definitions,” n.d.). Additionally, the European Data Protection Board (EDPB) Guidelines, such as Guideline 05/2020 on “consent” and the guidance on “legitimate interest,” offer valuable reference models for developing similar frameworks in Vietnam.

Providing Support and Tools for Small and Medium-Sized Enterprises (SMEs): To promote effective compliance and practical implementation of personal data protection among SMEs, the competent authority should adopt a range of supportive measures: (i) Tailored materials and tools: Develop user-friendly guidance documents, templates, and checklists that are adapted to the size and operational context of SMEs (“Home,” 2025). (ii) Training and knowledge sharing: Organize free or low-cost training programs and workshops to disseminate knowledge, share practical experiences, and address questions raised by SMEs. (iii) Online resource portal: Create a centralized digital platform that offers access to guidance materials, self-assessment tools, and downloadable compliance templates. (iv) Shared support mechanisms: Consider introducing a "shared DPO" model or subsidized legal advisory services for SMEs operating within the same sector or geographical area. (v) Risk-based approach: Allow

for simplified compliance obligations for low-risk data processing activities, provided that the fundamental rights of data subjects are still upheld.

Implementing a Comprehensive Awareness and Education Program on Personal Data Protection: To foster a society that is informed and proactive in protecting personal data, the responsible authority should implement a comprehensive education and communication program with the following key components ("Data Privacy Week - National Cybersecurity Alliance," n.d.): (i) Mass media campaigns: Utilize diverse communication channels including television, radio, social media, and print media to raise public awareness about data rights, common risks, and practical steps individuals can take to protect their data. (ii) Integration into education systems: Include privacy and data protection topics in school and university curricula to build awareness from an early age. (iii) Collaboration with civil society organizations (CSOs) and businesses: CSOs can play a crucial role in reaching marginalized or specific community groups. Businesses, especially e-commerce platforms, can integrate privacy information and guidance into their user interfaces to educate consumers. (iv) Development of interactive tools: Create mobile apps, educational games, or online tools to engage the public, particularly young people, in learning about privacy rights in an accessible and engaging way. Besides, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: Emphasize the critical importance of education and public awareness as part of a comprehensive privacy strategy ("OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 2002).

Enhancing International Cooperation and Adopting the Principle of Extraterritoriality: To augment enforcement efficacy and ensure the robust protection of personal data within a globalized milieu, it is imperative for Vietnam to proactively foster international cooperation and establish a legal framework congruent with established international norms and practices. This entails the following measures: (i) Engagement in International Cooperation Agreements: Vietnam should pursue the conclusion of Mutual Legal Assistance Treaties (MLATs) and other pertinent bilateral or multilateral agreements concerning data protection and inter-state law enforcement assistance ("The Council of Europe," n.d.). (ii) Accession to Regional and Global Frameworks: Consideration should be given to acceding to established mechanisms such as the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system ("Asia-Pacific Economic Cooperation," 2025). Such participation would facilitate secure

and transparent cross-border data flows, underpinned by cooperative enforcement mechanisms. (iii) Adoption of Extraterritorial Scope: Analogous to Article 3 of the GDPR ("Regulation - 2016/679 - EN - gdpr - EUR-Lex," n.d.), Vietnamese data protection legislation should extend its jurisdictional reach to foreign entities under circumstances where such entities:(1) Offer goods or services to data subjects in Vietnam, irrespective of whether a payment is required; or (2) Monitor the behavior of data subjects, insofar as their behavior takes place within Vietnam. (iv) Mandating the Appointment of a Local Representative: Foreign entities that do not have a physical establishment in Vietnam but engage in the processing of personal data of data subjects in Vietnam should be mandated to appoint a representative within Vietnam. This requirement, mirroring Article 27 of the GDPR, is crucial for enhancing supervisory oversight and domestic enforcement capabilities.

5 CONCLUSION AND POLICY IMPLICATIONS

This study has examined the evolving landscape of personal data protection in Vietnam's e-commerce sector, highlighting both legal advancements and practical implementation gaps. The enactment of Decree No. 13/2023/NĐ-CP represents a significant stride toward aligning national regulations with international standards such as the GDPR. However, the study reveals that enforcement remains inconsistent, especially among small and medium-sized enterprises (SMEs), and that public understanding of data rights is still limited.

Through thematic analysis and a SWOT framework, the research identifies critical areas of strength, such as legal momentum and growing consumer awareness, as well as persistent weaknesses, including regulatory ambiguity, lack of an independent enforcement authority, and resource constraints among key stakeholders. The findings underscore that data protection is not merely a technical or legal issue, but one that intersects with trust, digital literacy, business capability, and governance structure.

To bridge the gap between policy intent and practical effectiveness, the study proposes actionable recommendations: the establishment of an independent DPA, clearer and more operational legal definitions, targeted support mechanisms for SMEs, and a national public education campaign on data privacy. Furthermore, adopting international

cooperation mechanisms and principles of extraterritoriality will enhance Vietnam's ability to regulate cross-border data flows and hold foreign platforms accountable.

Ultimately, safeguarding personal data in the context of e-commerce is essential not only for ensuring consumer protection but also for fostering long-term trust, sustainable digital innovation, and international competitiveness. As Vietnam continues to digitize and integrate into the global digital economy, a rights-based, enforceable, and inclusive data protection regime will be fundamental to realizing its vision of a secure and resilient digital future.

REFERENCES

Ahmad, A., 2015. Business Intelligence for Sustainable Competitive Advantage, in: Advances in Business Marketing and Purchasing. Emerald Group Publishing Limited, pp. 3–220. https://doi.org/10.1108/S1069-096420150000022014

Art. 4 GDPR – Definitions, n.d. . General Data Protection Regulation (GDPR). URL https://gdpr-info.eu/art-4-gdpr/ (accessed 5.15.25).

Asia-Pacific Economic Cooperation [WWW Document], 2025. . APEC. URL https://apec.org (accessed 5.15.25).

Ceross, A., 2018. Examining data protection enforcement actions through qualitative interviews and data exploration. International Review of Law, Computers & Technology 32, 99–117. https://doi.org/10.1080/13600869.2018.1418143

Cho, J., Vo, T.H.G., Le, K.H., Luong, D.B., 2023. How to influence consumer behaviour: A perspective from E-commerce in Vietnam context. IJECS 14, 1–14. https://doi.org/10.7903/ijecs.2292

Choi, T., Wallace, S.W., Wang, Y., 2018. Big Data Analytics in Operations Management. Production and Operations Management 27, 1868–1883. https://doi.org/10.1111/poms.12838

Data Privacy Week - National Cybersecurity Alliance [WWW Document], n.d. URL https://www.staysafeonline.org/data-privacy-week (accessed 5.15.25).

Digital in Vietnam [WWW Document], n.d. . DataReportal – Global Digital Insights. URL https://datareportal.com/digital-in-vietnam (accessed 5.14.25).

eCommerce - Vietnam | Statista Market Forecast [WWW Document], n.d. . Statista. URL http://frontend.xmo.prod.aws.statista.com/outlook/emo/ecommerce/vietnam?utm_source=chatgpt.com (accessed 5.14.25).

European Parliament. Directorate General for Parliamentary Research Services., 2020. The impact of the general data protection regulation on artificial intelligence. Publications Office, LU.

Groenewald, D.E.S., 2024. E-commerce Inventory Auditing: Best Practices, Challenges, and the Role of Technology 1.

Hassan, N., Abdelraouf, M., El-Shihy, D., 2025. The moderating role of personalized recommendations in the trust–satisfaction–loyalty relationship: an empirical study of AI-driven e-commerce. Futur Bus J 11, 66. https://doi.org/10.1186/s43093-025-00476-z

Home [WWW Document], 2025. URL https://ico.org.uk/ (accessed 5.15.25).

Jack Trọng, 2024. Relationship between Data Privacy Regulations and Consumer Trust in E-Commerce Platforms in Vietnam. AJDIKM 5, 49–58. https://doi.org/10.47672/ajdikm.2347

Kumar, P., Mokha, A.K., Pattnaik, S.C., 2022. Electronic customer relationship management (E-CRM), customer experience and customer satisfaction: evidence from the banking industry. BIJ 29, 551–572. https://doi.org/10.1108/BIJ-10-2020-0528

Lee, W.W., Zankl, W., Chang, H., n.d. feature An Ethical Approach to Data Privacy Protection.

Morić, Z., Dakic, V., Djekic, D., Regvart, D., 2024. Protection of Personal Data in the Context of E-Commerce. JCP 4, 731–761. https://doi.org/10.3390/jcp4030034

Neta, Y., Awanisa, A., Melisa, M., 2022. The Urgency of Establishing Independent Supervisory Authority for Personal Data Protection in Indonesia. Constitutionale 3, 19–38. https://doi.org/10.25041/constitutionale.v3i1.2535

NGUYEN, C.Q., CHUNG, L.P., 2022. What Determines the Online Shopping Intention of Vietnamese Consumers? East Asian Journal of Business Economics (EAJBE) 10, 19–30. https://doi.org/10.20498/EAJBE.2022.10.2.19

Nguyen, L.M., Long, L.V., Nam, T.V., Chen, T.H., 2024. PERSONAL DATA IN THE DIGITAL AGE: AN OVERVIEW STUDY IN VIETNAM. J. of Law and Sust. Develop. 12, e2623. https://doi.org/10.55908/sdgs.v12i3.2623

Norberg, P.A., Horne, D.R., Horne, D.A., 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. Journal of Consumer Affairs 41, 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Nouwens, M., Kristensen, J.B., Maalt, K., Bagge, R., 2025. A Cross-Country Analysis of GDPR Cookie Banners and Flexible Methods For Scraping Them, in: Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems. Presented at the CHI 2025: CHI Conference on Human Factors in Computing Systems, ACM, Yokohama Japan, pp. 1–28. https://doi.org/10.1145/3706598.3713648

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [WWW Document], 2002. . OECD. URL https://www.oecd.org/en/publications/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.html (accessed 5.15.25).

Proserpio, D., Zervas, G., 2017. Online Reputation Management: Estimating the Impact of Management Responses on Consumer Reviews. Marketing Science 36, 645–665. https://doi.org/10.1287/mksc.2017.1043

Quach, S., Thaichon, P., Martin, K.D., Weaven, S., Palmatier, R.W., 2022. Digital technologies: tensions in privacy and data. J. of the Acad. Mark. Sci. 50, 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

Raj, R., Singh, A., Kumar, V., De, T., Singh, S., 2024. Assessing the e-commerce last-mile logistics' hidden risk hurdles. Cleaner Logistics and Supply Chain 10, 100131. https://doi.org/10.1016/j.clscn.2023.100131

Regulation - 2016/679 - EN - gdpr - EUR-Lex [WWW Document], n.d. URL https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (accessed 5.15.25).

Schäfer, F., Gebauer, H., Gröger, C., Gassmann, O., Wortmann, F., 2023. Data-driven business and data privacy: Challenges and measures for product-based companies. Business Horizons 66, 493–504. https://doi.org/10.1016/j.bushor.2022.10.002

softcircles, n.d. 10 Best Practices to Creating Powerful Sign-up Forms for e-commerce website [WWW Document]. softcircles. URL https://softcircles.com/blog/aical.html (accessed 6.8.25).

Sulastri, L., 2023. The Role of Artificial Intelligence in Enhancing Customer Experience: A Case Study of Global E-commerce Platforms. IJSOC 5, 451–469. https://doi.org/10.54783/ijsoc.v5i3.1257

The Council of Europe: guardian of Human Rights, Democracy and the Rule of Law for 700 million citizens - Portal - www.coe.int [WWW Document], n.d. . Portal. URL https://www.coe.int/en/web/portal (accessed 5.15.25).

thuvienphapluat.vn, n.d. 13/2023/ND-CP in Vietnam, Decree No. 13/2023/ND-CP dated April 17, 2023 on protection of personal data in Vietnam [WWW Document]. THƯ VIỆN PHÁP LUẬT. URL https://thuvienphapluat.vn/van-ban/EN/Cong-nghe-thong-tin/Decree-No-13-2023-ND-CP-dated-April-17-2023-on-protection-of-personal-data/564343/tieng-anh.aspx (accessed 5.13.25).

Trade W.P.M. of I., n.d. Web Portal Ministry of Industry and Trade [WWW Document]. moit.gov.vn. URL http://moit.gov.vn (accessed 5.14.25).

Viu-Roig, M., Alvarez-Palau, E.J., 2020. The Impact of E-Commerce-Related Last-Mile Logistics on Cities: A Systematic Literature Review. Sustainability 12, 6492. https://doi.org/10.3390/su12166492

White Book of Viet Nam Information and Communication Technology 2023 [WWW Document], n.d. URL https://mic.gov.vn/bao-giay/white-book-of-viet-nam-information-and-communication-technology-2023-73.htm (accessed 5.14.25).

Yong, S.C.S.C., Huan, R.T., Poh, W.S., Osman, M., Ng, D.C.W., 2023. Assessing the Factors Influencing Consumer Behaviour in E-Commerce Platforms. IJMABER 4, 3725–3735. https://doi.org/10.11594/ijmaber.04.10.25

Zhang, Z., Yin, H., Rao, S.X., Yan, X., Wang, Z., Liang, W., Zhao, Y., Shan, Y., Zhang, R., Lin, Y., Jiang, J., 2025. Identifying E-Commerce Fraud Through User Behavior

Data: Observations and Insights. Data Sci. Eng. 10, 24–39. https://doi.org/10.1007/s41019-024-00275-6

Authors Declarations and Essential Ethical Compliances:

The author is solely responsible for all aspects of this work, including conception, design, data collection, analysis, and manuscript writing.

Funding: This study forms part of the author doctoral dissertation carried out during the PhD program at the University of Law, Ho Chi Minh City, Vietnam.

Research involving human bodies or organs or tissues (Helsinki Declaration): The author(s) solemnly declare(s) that this research has not involved any human subject (body or organs) for experimentation. It was not clinical research. The contexts of human population/participation were only indirectly covered through literature review. Therefore, an Ethical Clearance (from a Committee or Authority) or ethical obligation of Helsinki Declaration does not apply in cases of this study or written work. Research involving animals (ARRIVE Checklist): The author(s) solemnly declare(s) that this research has not involved any animal subject (body or organs) for experimentation. The research was not based on laboratory experiment involving any kind animal. The contexts of animals were only indirectly covered through literature review. Therefore, an Ethical Clearance (from a Committee or Authority) or ethical obligation of ARRIVE does not apply in cases of this study or written work.

Research on Indigenous Peoples and/or Traditional Knowledge: The author solemnly declare(s) that this research has not involved Indigenous Peoples as participants or respondents. The contexts of Indigenous Peoples or Indigenous Knowledge were only indirectly covered through literature review. Therefore, an Ethical Clearance (from a Committee or Authority) or prior informed consent (PIC) of the respondents or Self Declaration in this regard does not apply in cases of this study or written work.

Research involving Plants: The author(s) solemnly declare(s) that this research has not involved the plants for experiment and field studies. Some contexts of plants are also indirectly covered through literature review. Thus, during this research the author(s) obeyed the principles of the Convention on Biological Diversity and the Convention on the Trade in Endangered Species of Wild Fauna and Flora.

Research Involving Local Community Participants (Non-Indigenous) or Children: The author(s) solemnly declare(s) that this research has not directly involved any local

community participants or respondents belonging to non-Indigenous peoples. Neither this study involved any child in any form directly. The contexts of different humans, people, populations, men/women/children and ethnic people were only indirectly covered through literature review. Therefore, an Ethical Clearance (from a Committee or Authority) or prior informed consent (PIC) of the respondents or Self-Declaration in this regard does not apply in cases of this study or written work.

PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses): The author(s) has/have NOT complied with PRISMA standards. It is not relevant in case of this study or written work.

Competing Interests/Conflict of Interest: Author(s) has/have no competing financial, professional, or personal interests from other parties or in publishing this manuscript. There is no conflict of interest with the publisher or the editorial team or the reviewers.

Attribution and Representation: All opinions and mistakes are the author(s)' own and cannot be attributed to the institutions they represent. The publisher is also not responsible either for such opinions and mistakes in the text or graphs or images.

Declaration of the Use of AI: During the preparation of this work, the authors have used AI [Deep Sense] to assists the script translation and proof reading. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the published article.

Authors' Contribution

Both authors contributed equally to the development of this article.

Data availability

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

How to cite this article (APA):

Minh, N. L., & Binh, H. T. T. ENHANCING PERSONAL DATA PROTECTION ON E-COMMERCE PLATFORMS: A CASE STUDY IN VIETNAM. Veredas Do Direito, e223116 . https://doi.org/10.18623/rvd.v22.n2.3116