NHO LE

Sustainable Consumer Data Protection in Vietnam's E-Commerce: Bridging Legal Gaps Through Global Insights

Abstract

Vietnam's enactment of the Personal Data Protection Law (PDPL), in 2025, scheduled to enter into force in 2026, represents a landmark shift toward codifying a modern data protection regime. Yet, the law enters a digital marketplace dominated by data-driven e-commerce platforms, uneven institutional capacities, and fragmented regulatory frameworks. This paper examines whether the PDPL can meaningfully safeguard consumer personal data in Vietnam's rapidly expanding e-commerce sector, and what legal, institutional, and comparative insights can support its sustainable implementation. Drawing on a structured comparative analysis of the EU's GDPR, China's PIPL, and California's CCPA, the paper evaluates how different regulatory philosophies, including rights-based, state-centric, and market-driven, offer lessons for refining Vietnam's approach. Building on doctrinal, comparative, and normative analysis, the paper identifies persistent gaps in enforcement independence, lawful bases for processing, cross-border data governance, and sector-specific guidance for e-commerce. It proposes a sustainability-oriented, multi-dimensional reform framework emphasizing institutional independence, regulatory harmonization, risk-based governance, and sustainable data stewardship. The paper contributes to theoretical debates on consumer data governance in emerging economies, and provides policy guidance for Vietnam as it seeks to build a trustworthy, rights-respecting, and sustainable digital market.

KEYWORDS: consumer data protection, e-commerce, GDPR; personal data governance, Vietnam PDPL

NHO LE – MA in law, Ho Chi Minh City Open University,
ORCID – 0000-0002-8330-9104, e-mail: lenho77@gmail.com

HTTPS://DOI.ORG/10.36128/19CD0230

1 Introduction

Vietnam's digital economy has experienced unprecedented growth over the past decade, driven largely by the proliferation of e-commerce platforms and data-driven transactional models. Personal data has increasingly become the central asset enabling targeted advertising, personalized recommendations, and dynamic pricing, thereby reshaping consumer interaction in online environments.[1] Yet these same practices expose consumers to heightened vulnerabilities, including unauthorized data sharing, opaque profiling, and cross-border risks.

The enactment of the Personal Data Protection Law (PDPL) in 2025 marks Vietnam's first comprehensive legislative effort to consolidate dispersed rules into a unified statutory regime.[2] Compared to earlier frameworks – primarily embodied in Decree No. 13/2023/ND-CP – the PDPL introduces more robust legal definitions, explicit rights for data subjects, monetary penalties, and obligations for high-risk processing. However, its alignment with actual data-intensive commercial practices remains uncertain, particularly in e-commerce settings dominated by private platforms, multinational service operators, and third-party data brokers.

Existing scholarship on Vietnam's data protection reform has mainly assessed the transition toward codification and examined similarities with the GDPR.[3] However, limited academic literature directly addresses how the PDPL functions within e-commerce and how consumer data – distinct from general personal data – is regulated through consent-based or risk-based governance. Furthermore, sustainability implications remain underexplored. In digital markets, the protection of consumer data contributes not only to privacy assurance but also to sustainable commercial trust and long-term market fairness, themes that have not received systematic attention.

---

1 Viktor Mayer-Schönberger, Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Boston: Houghton Mifflin Harcourt, 2013); Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford: Oxford University Press, 2019); Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).

2 National Assembly of Vietnam, *Personal Data Protection Law* (adopted June 2025, effective January 2026).

3 Graham Greenleaf, "Vietnam's 2024 Draft Data Privacy Law Is Ambitious and Ambiguous" *Privacy Laws & Business International Report*, 192 (2024): 22-25.

This paper addresses three major questions. First, how does the PDPL currently regulate consumer personal data in e-commerce contexts? Second, what structural and institutional gaps continue to constrain enforcement and operational clarity? Third, what comparative insights from the GDPR, PIPL, and CCPA can support Vietnam's next reform stage?

This paper makes three contributions. Doctrinally, it provides one of the first structured assessments of the PDPL, specifically through an e-commerce lens. Conceptually, it distinguishes consumer data from general personal data and situates this distinction within sustainability-oriented regulatory theory. Normatively, it proposes a reform framework grounded in comparative lessons but adapted to Vietnam's institutional realities, emphasizing enforcement independence, risk-based governance, and cross-border compatibility.

The remainder of the paper proceeds as follows. Section 2 reviews relevant research on consumer data and digital governance. Section 3 analyzes how the PDPL regulates consumer personal data in e-commerce. Section 4 conducts a comparative analysis of GDPR, PIPL, and CCPA. Section 5 proposes policy recommendations and outlines a reform roadmap. Section 6 concludes.

2 Literature Review: Consumer Data, Privacy, and E-Commerce Governance

Research on data governance is well-established across interdisciplinary domains, especially law, economics, behavioral studies, and digital sociology. Three major strands of research provide theoretical grounding for this paper.

Contemporary data-driven markets are shaped by the commodification of user information and the strategic use of transactional data for behavioral analytics, profiling, and predictive market segmentation. Scholars identify personal data as the core extractive resource enabling surveillance-oriented and hyper-personalized commercial systems.[4] A second

[4] Ben Wagner, *Algorithmic Regulation* (Oxford: Oxford University Press, 2022); Zuboff, *The Age of Surveillance Capitalism*; Cohen, *Between Truth and Power*; Evgeny

line of research emphasizes how platforms capture value asymmetrically through algorithmic categorization, behavioral nudging, and monetization of metadata, ultimately reinforcing market power in digital ecosystems. Although these perspectives offer sophisticated explanations of data-centric markets, they have not been fully examined in emerging regulatory systems such as Vietnam, where legal frameworks have historically lagged behind technological innovation.

Data protection regimes differ fundamentally in their regulatory philosophies and institutional outcomes. Comparative legal scholarship distinguishes between rights-based approaches (EU), security-based approaches (China), and market-based approaches (United States). A large body of work compares the institutional design and enforcement structure under these regimes, emphasizing how their normative foundations filter into compliance obligations and business incentives.[5] However, existing comparative studies rarely extend into examining how hybrid models could be applied in a transitional economy with multi-layered regulation such as Vietnam, especially for e-commerce-specific data clusters involving tracking, profiling, cross-border storage, and real-time monetization.

Prior studies of Vietnam's regulatory development highlight an uneven progression toward comprehensive rules, shifting from overlapping ministerial circulars and decrees into nationwide statutory legislation. Discussions frequently address problems of dispersed authorities, lack of unified definitions, or insufficient enforcement mechanisms. Yet these studies often treat personal data as a homogeneous legal category rather than consumer-specific data generated through online commerce.[6] Little research articulates how data protection contributes to broader policy goals such as digital trust, sustainable e-commerce development, and consumer fairness, an academic gap that this paper addresses through a sustainability-oriented governance framework.

Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism* (New York: PublicAffairs, 2013).

5 Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford: Oxford University Press, 2013); Igor Calzada, "Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)" *Smart Cities*, No. 3 (2022): 1129-1150. https://doi.org/10.3390/smartcities5030057; Daniel J. Solove, Woodrow Hartzog, "The Scope and Potential of FTC Data Protection" *George Washington Law Review*, 83 (2015): 2230-2273.

6 Tố Trang Lam, "Some Legal Aspects of Personal Data Protection in the World – Experience for Vietnam," *Cogent Social Sciences*, No. 1 (2024); Greenleaf, "Vietnam's 2024 Draft Data Privacy Law."

3 Conceptual and Legal Foundations of Consumer Data Protection

3.1. Personal Data and Consumer Data: Distinction and Overlap

Personal data is commonly understood as information relating to an identified or identifiable natural person, regardless of the context in which such information is generated or processed.[7] This broad and technology-neutral concept forms the cornerstone of contemporary data protection regimes, including the GDPR and Vietnam's Personal Data Protection Law (PDPL). By framing personal data as a general legal category, these regimes seek to ensure baseline protection for individual autonomy and informational dignity across diverse social, administrative, and commercial settings.[8]

Within this broad category, consumer data represents a context-specific subset of personal data generated through commercial interactions between individuals and market actors. Consumer data typically encompasses transactional records, purchasing histories, browsing behavior, preference signals, and inferred profiles derived from online interactions on digital platforms.[9] Unlike general personal data, consumer data is intrinsically linked to market asymmetries, profit-driven processing, and behavioral influence strategies, particularly in e-commerce environments characterized by large-scale data aggregation and automated decision-making.[10]

The distinction between personal data and consumer data, however, is not absolute. While all consumer data qualifies as personal data under prevailing legal definitions, not all personal data carries the same economic function or regulatory risk profile. The overlap between these categories creates regulatory challenges, especially when general data protection rules are applied uniformly to consumer-generated datasets without accounting for their commercial sensitivity and potential for manipulation. Failure to acknowledge this overlap may result in formalistic consent

7 Christopher Millard, W. Kuan Hon, "Defining 'Personal Data' in e-Social Science" *Information, Communication & Society*, 15 (2011).

8 Regulation (EU) 2016/679 (General Data Protection Regulation), art. 4(1); National Assembly of Vietnam, *Personal Data Protection Law*, arts. 2-3; Solove, Hartzog, "The Scope and Potential of FTC Data Protection."

9 Rahmi Ayunda, "Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties?" *Law Reform*, No. 2 (2022): 144-163.

10 OECD, "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value" OECD Digital Economy Papers, No. 220 (2013).

mechanisms, insufficient safeguards against profiling, and weak oversight of downstream data sharing practices in digital markets.

3.2. Intersection between Privacy, Data Protection, and Consumer Protection

Privacy traditionally reflects a normative and rights-based concept concerned with individual autonomy, dignity, and control over personal life.[11] In legal theory, privacy functions as a foundational value rather than a purely regulatory tool, shaping the ethical boundaries of information use and surveillance.[12] Within digital environments, privacy interests are increasingly challenged by continuous data extraction, behavioral monitoring, and opaque commercial practices that extend beyond the individual's immediate awareness or consent.

Data protection, by contrast, operates as a procedural and institutional framework designed to operationalize privacy through concrete obligations imposed on data controllers and processors.[13] Rather than safeguarding privacy as an abstract right, data protection law focuses on governance mechanisms such as consent requirements, purpose limitation, accountability, risk assessment, and supervisory oversight. In this sense, data protection serves as the primary legal instrument through which privacy principles are translated into enforceable compliance duties within both public and private sectors.

Consumer protection law introduces a distinct regulatory logic by addressing information asymmetries, unfair commercial practices, and contractual imbalances in market transactions.[14] Unlike privacy and data protection regimes, consumer protection frameworks are explicitly

11 Lam, "Some Legal Aspects of Personal Data Protection in the World – Experience for Vietnam."

12 Daniel J. Solove, *Understanding Privacy* (Cambridge: Harvard University Press, 2008).

13 European University Institute, *Guide on Good Data Protection Practice in Research* (Florence: European University Institute, 2022), 5.

14 Archana Goel, Utkal Khandelwal, Jayalakshmy Ramachandran, "Three Decades of Consumer Protection Literature: Systematic Review and Future Research Agenda" *Journal of Creative Communications* (2025); Nguyen Duy Phuong, Nguyen Duy Thanh, "Law on Corporate Social Responsibility for Consumers in Vietnam" *Prawo i Więź*, No. 1 (2022): 297-312.

market-oriented, aiming to ensure transparency, fairness, and effective remedies in commercial relationships. In digital commerce, consumer protection norms increasingly intersect with data governance, particularly where personal data functions as a form of counter-performance in exchange for access to online services or price advantages.

The intersection of privacy, data protection, and consumer protection reveals significant regulatory tension in e-commerce governance. While data protection regimes emphasize procedural legality and consent, consumer protection law demands substantive fairness and protection against manipulation. In Vietnam, these frameworks largely operate in parallel rather than as an integrated regulatory matrix, resulting in fragmented oversight of consumer data practices on digital platforms. This fragmentation weakens protection against profiling-based exploitation, dynamic pricing discrimination, and opaque data-driven marketing strategies, underscoring the need for coordinated governance across legal domains.

3.3. Risks Arising from E-Commerce-Driven Data Ecosystems

E-commerce platforms operate as data-intensive ecosystems in which consumer interactions are continuously recorded, aggregated, and analyzed across multiple layers of digital infrastructure. These ecosystems generate a wide range of risks that extend beyond traditional data security concerns, including pervasive behavioral monitoring, large-scale profiling, and algorithmic influence over consumer choice. Such risks are amplified by the integration of third-party analytics services, advertising networks, and cross-platform tracking technologies that obscure data flows from end users.[15]

These risks are structurally produced by the commercial logic underpinning platform-driven digital markets. Real-time data collection enables predictive analytics, dynamic pricing, and personalized recommendation systems that can subtly shape consumer behavior while remaining largely invisible to affected individuals. The reliance on inferred data – such as predictive preferences, risk scores, and consumption propensities – further

15 Shoshana Zuboff, *The Age of Surveillance Capitalism* (New York: PublicAffairs, 2019); Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford: Oxford University Press, 2019).

intensifies regulatory challenges, as these data points are rarely disclosed, contested, or meaningfully consented to by consumers.[16]

From a legal perspective, e-commerce-driven data risks raise concerns that cannot be fully addressed through consent-based compliance alone. Algorithmic profiling may lead to discriminatory outcomes, informational manipulation, and unequal market access, particularly where consumers lack effective mechanisms to understand, challenge, or opt out of automated decision-making processes.[17] In jurisdictions with fragmented regulatory oversight, such as Vietnam, these risks expose gaps in accountability, enforcement coordination, and substantive fairness protections, highlighting the need for sector-specific governance approaches tailored to digital commerce.

3.4. PDPL's Normative Model and its Practical Implications

Vietnam's Personal Data Protection Law (PDPL) adopts a predominantly consent-based normative model, positioning individual consent as the primary legal ground for lawful data processing. This model reflects an intention to affirm personal autonomy and individual control over personal data, while introducing baseline obligations such as purpose limitation, data minimization, and risk-based impact assessments for high-risk processing activities.[18] In doctrinal terms, the PDPL aligns with a rights-oriented conception of data protection, emphasizing formal legality and procedural compliance as central regulatory objectives.

Despite these normative commitments, the PDPL's implementation framework reveals significant practical limitations in data-intensive commercial environments. The absence of an explicit "legitimate interests" ground, combined with limited guidance on profiling, inferred data, and automated decision-making, encourages platforms to rely on layered consent mechanisms rather than substantive risk mitigation.[19] As a result,

16 Ben Wagner, *Algorithmic Regulation* (Oxford: Oxford University Press, 2022); OECD, "Exploring the Economics of Personal Data".

17 Solove, Hartzog, "The Scope and Potential of FTC Data Protection"; Graham Greenleaf, "Vietnam's 2024 Draft Data Privacy Law Is Ambitious and Ambiguous."

18 Graham Greenleaf, "Vietnam's 2024 Draft Data Privacy Law Is Ambitious and Ambiguous" *Privacy Laws & Business International Report*, 192 (2024): 22-25.

19 Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford: Oxford University Press, 2013); Calzada, "Citizens' Data Privacy in China: The State of the Art of

compliance strategies often prioritize disclosure formalities over meaningful governance redesign, leaving underlying asymmetries in data-driven market power largely unaddressed.

At the system level, these implementation gaps have important implications for e-commerce governance in Vietnam. A consent-centric regulatory architecture may inadvertently normalize excessive data extraction, while shifting the burden of protection onto consumers who lack the informational capacity to assess complex data practices.[20] Without clearer standards for accountability, proportionality, and enforceable safeguards against abusive profiling, the PDPL risks functioning as a procedural compliance framework rather than a mechanism for substantive consumer data protection. This limitation calls for a broader governance-oriented approach to consumer data protection. These challenges underscore the need to complement consent-based rules with structural governance tools tailored to platform-driven digital markets.

3.5. Sustainable Data Protection as a Governance Principle

The concept of sustainable data protection has emerged in contemporary regulatory scholarship as a response to the limitations of purely procedural and consent-based data governance models. Rather than focusing exclusively on short-term compliance obligations, sustainable data protection emphasizes long-term accountability, proportionality, institutional resilience, and the alignment of data practices with broader social and economic objectives. In this sense, sustainability functions not merely as a policy aspiration but as a governance principle guiding the design and evaluation of data protection regimes in digital economies.[21]

Applied to consumer data governance, sustainability requires regulators to move beyond individual consent as the sole legitimizing mechanism for data processing. Sustainable frameworks prioritize structural safeguards, including transparency by design, limits on excessive data extraction,

---

the Personal Information Protection Law (PIPL)."

20 Francesca Casalini, Javier López González, "Trade and Cross-Border Data Flows" *OECD Trade Policy Papers*, No. 220 (2019).

21 European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Shaping Europe's Digital Future*, COM(2020) 67 final, 19 February 2020; Casalini, González, *Trade and Cross-Border Data Flows*.

meaningful oversight of profiling practices, and mechanisms that reduce informational asymmetries between platforms and consumers.[22] These elements are particularly relevant in e-commerce environments, where data-driven business models operate continuously and at scale, generating cumulative risks that cannot be effectively mitigated through isolated consent decisions.

For Vietnam, adopting sustainable data protection as a governance principle offers a conceptual foundation for refining the PDPL's implementation in line with international best practices, while remaining sensitive to domestic regulatory capacity. By embedding sustainability-oriented criteria – such as proportionality, accountability, and institutional coordination – into consumer data regulation, Vietnam can better address systemic risks associated with platform dominance, cross-border data flows, and algorithmic decision-making. This governance-oriented perspective also provides a coherent analytical bridge to comparative regulatory models examined in the following section.

4 Comparative Analysis of Consumer Data Protection Frameworks

Comparative assessments of global data protection frameworks reveal meaningful contrasts in regulatory philosophies, legal obligations, enforcement structures, and mechanisms for consumer rights protection. These contrasts provide important reference points for Vietnam as it seeks to operationalize the PDPL in a complex and rapidly evolving e-commerce environment.

22 Ben Wagner, *Algorithmic Regulation* (Oxford: Oxford University Press, 2022); Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford: Oxford University Press, 2019).

4.1. Regulatory Philosophy and Normative Foundations

The GDPR is grounded in a rights-based regulatory philosophy rooted in European constitutional traditions, treating personal data protection as an extension of fundamental rights to privacy, dignity, and informational self-determination. This normative foundation emphasizes proportionality, accountability, and the balancing of competing interests, allowing data processing to be justified not only through consent but also through legitimate interests and public policy considerations. As a result, the GDPR conceptualizes consumer data protection as part of a broader human rights architecture rather than a purely market-regulatory instrument.[23]

In contrast, China's Personal Information Protection Law (PIPL) reflects a governance philosophy centered on state supervision, cybersecurity, and social stability. While the PIPL formally recognizes individual rights, its regulatory logic prioritizes systemic risk management, data localization, and administrative control over data-intensive industries.[24] Consumer data protection under the PIPL thus operates within a security-oriented framework that emphasizes ex ante control and state oversight rather than judicially mediated balancing of interests.

The California Consumer Privacy Act (CCPA) adopts a markedly different normative orientation, grounded in market transparency and consumer choice rather than comprehensive rights protection. Its emphasis on notice, opt-out mechanisms, and limited purpose restrictions reflects a pragmatic attempt to correct information asymmetries without fundamentally restructuring data-driven business models. Consumer data is treated primarily as a commercial asset subject to disclosure obligations, positioning consumer autonomy within a transactional logic.[25]

Vietnam's PDPL exhibits a hybrid normative character, borrowing rights-based language from the GDPR while operationally relying on a consent-centric model closer to transactional approaches. However, unlike the GDPR, the PDPL lacks explicit balancing mechanisms or alternative lawful

23 GDPR, Charter of Fundamental Rights of the European Union, OJ C 326, 26 October 2012, arts 7-8; Kuner, *Transborder Data Flows and Data Privacy Law*.

24 Igor Calzada, "Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)" *Smart Cities*, No. 3 (2022): 1129-1150.

25 California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq.

bases for processing, limiting its capacity to address consumer data risks in complex e-commerce ecosystems.[26]

4.2. Enforcement Architecture and Institutional Design

Effective consumer data protection depends not only on substantive rights but also on institutional enforcement design. Under the GDPR, independent supervisory authorities (DPAs) play a central role in interpreting norms, coordinating cross-border enforcement, and imposing sanctions.[27] This institutional independence enhances regulatory credibility and ensures that consumer data protection is insulated from short-term political or commercial pressures.

By contrast, enforcement under the PIPL is centralized within state administrative agencies with broad discretionary powers. While this model enables swift regulatory intervention, it also concentrates interpretive authority and limits avenues for adversarial challenge by consumers or firms. Consumer protection is thus mediated through administrative governance rather than rights-based adjudication.[28]

The CCPA relies on a mixed enforcement architecture, combining regulatory oversight by the California Privacy Protection Agency (CPPA) with private enforcement mechanisms in limited circumstances.[29] This structure prioritizes regulatory guidance, standardized compliance tools, and accessibility for consumers, albeit at the cost of narrower substantive protections.

Vietnam's PDPL currently adopts a centralized enforcement model similar to the PIPL, with oversight vested in a single executive authority.[30] The absence of an independent supervisory body or sector-specific regulators constrains enforcement diversity and limits the development of specialized

26 Graham Greenleaf, "Vietnam's 2024 Draft Data Privacy Law Is Ambitious and Ambiguous" *Privacy Laws & Business International Report*, 192 (2024): 22-25.

27 European Union, *Regulation (EU) 2016/679 — General Data Protection Regulation (GDPR)*, arts. 51–58 (2016).

28 Gulbakyt Bolatbekkyzy, "Comparative Insights from the EU's GDPR and China's PIPL for Advancing Personal Data Protection Legislation," *Groningen Journal of International Law*, 11 (2024): 129-146.

29 California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.199.10 (establishing the enforcement authority of the California Privacy Protection Agency).

30 Lam, "Some Legal Aspects of Personal Data Protection in the World – Experience for Vietnam."

consumer data governance expertise, particularly in fast-evolving digital markets.

4.3. Lawful Bases for Processing and Consumer Autonomy

The GDPR's pluralistic framework of lawful processing bases – including consent, legitimate interests, contractual necessity, and legal obligations – provides regulatory flexibility in commercial contexts.[31] This structure allows consumer data processing to be assessed through proportionality and necessity tests rather than relying exclusively on formal consent.

The PIPL permits processing without consent in limited circumstances tied to statutory duties, public interests, or emergency situations, reflecting its security-oriented logic.[32] Although narrower than the GDPR's framework, these exceptions acknowledge the limitations of consent in large-scale data ecosystems.

The CCPA operationalizes consumer autonomy primarily through opt-out rights, particularly concerning data sales and targeted advertising.[33] While this approach enhances practical accessibility, it places the burden of protection on consumers and offers limited safeguards against profiling and inferred data practices.

Vietnam's PDPL, by contrast, relies almost exclusively on consent as the legal basis for consumer data processing.[34] This approach risks overburdening consumers with complex disclosure requirements, while allowing data-intensive platforms to legitimize extensive processing through procedural compliance rather than substantive justification.

31 GDPR arts. 6-7.
32 PIPL arts. 13-15.
33 CCPA §1798.120.
34 PDPL consent provisions.

4.4. Consumer Rights, Redress Mechanisms, and Accessibility

Under the GDPR, consumer rights such as access, rectification, erasure, and objection are reinforced by procedural guarantees, response deadlines, and oversight by supervisory authorities.[35] These mechanisms transform abstract rights into actionable protections within digital markets.

The CCPA emphasizes usability and interface-based rights execution, requiring businesses to provide clear mechanisms for submitting requests and opting out of data sales. [36] While substantively narrower, this design enhances practical consumer engagement with data rights.

The PIPL recognizes individual rights but channels enforcement primarily through administrative oversight, limiting the role of private complaints and judicial remedies.[37] Consumer redress thus depends heavily on regulatory discretion rather than individual empowerment.

Vietnam's PDPL formally recognizes consumer rights but lacks standardized procedures, timelines, and digital interfaces for their exercise. This gap weakens the practical effectiveness of consumer data rights in e-commerce settings, where scale and automation demand accessible remedies.[38]

4.5. Cross-Border Data Transfers and Platform Accountability

Cross-border data governance constitutes a critical dimension of consumer data protection in global e-commerce. The GDPR employs adequacy decisions, standard contractual clauses, and binding corporate rules to manage cross-border transfers, while maintaining rights equivalence.[39]

---

35 GDPR arts. 12-22; European Data Protection Board, *Guidelines 01/2022 on Data Subject Rights – Right of Access* (adopted 28 March 2023), European Data Protection Board. https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf.

36 California Privacy Protection Agency, *California Consumer Privacy Act Regulations* (effective January 2, 2024), §§ 7013–7020 (requiring clear opt-out mechanisms and consumer request submission interfaces), https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf.

37 PIPL rights provisions.

38 PDPL; Greenleaf.

39 GDPR Chapter V.

The PIPL adopts a more restrictive approach, requiring security assessments and data localization in certain circumstances, reflecting concerns over national security and regulatory control.[40]

The CCPA relies primarily on contractual and transparency-based mechanisms, emphasizing disclosure rather than substantive transfer restrictions.[41]

Vietnam's PDPL requires notification and risk assessments for certain cross-border transfers but lacks interoperable mechanisms comparable to adequacy or mutual recognition frameworks.[42] This creates uncertainty for multinational e-commerce platforms and limits Vietnam's integration into global digital trade regimes.

Taken together, the comparative analysis demonstrates that effective consumer data protection in digital markets depends on more than the formal recognition of individual rights. Jurisdictions that combine pluralistic lawful processing bases, diversified enforcement architectures, and sector-specific safeguards are better equipped to address the structural risks posed by data-intensive e-commerce ecosystems. These comparative insights provide an analytical foundation for assessing how Vietnam's PDPL can evolve toward a more sustainable and resilient consumer data protection framework.

5 Toward a Sustainable Consumer Data Protection Framework for Vietnam

5.1. Reframing Consumer Data Protection through Sustainability

Conventional approaches to consumer data protection in Vietnam have largely emphasized formal compliance, particularly through consent-based obligations and procedural disclosures. While these mechanisms establish a baseline of legality, they are insufficient to address cumulative and systemic risks generated by data-intensive e-commerce ecosystems. A sustainability-oriented framework requires a shift from short-term

40 PIPL cross-border transfer rules.
41 CCPA disclosure framework.
42 PDPL, art. 20.

compliance towards long-term governance objectives, including proportionality, accountability, institutional resilience, and market fairness.[43]

Under this perspective, consumer data protection is no longer treated as an isolated individual right but as a structural component of sustainable digital market regulation. Sustainability thus functions as an evaluative criterion, enabling regulators to assess whether data practices contribute to or undermine consumer trust, competitive neutrality, and long-term economic stability.

5.2. Institutional Sustainability: Diversifying Enforcement and Oversight

Institutional design constitutes a foundational element of sustainable consumer data protection. As demonstrated in Section 4, jurisdictions with diversified enforcement architectures – such as independent supervisory authorities or sector-specific regulators – exhibit greater regulatory adaptability and enforcement credibility. Vietnam's centralized enforcement model, while administratively efficient, constrains institutional learning and limits the development of specialized oversight capacity for complex e-commerce practices.

To enhance institutional sustainability, Vietnam could consider establishing a semi-independent supervisory mechanism for consumer-facing data practices, supported by inter-agency coordination with competition and consumer protection authorities. Such diversification would strengthen accountability, reduce regulatory blind spots, and enable more responsive governance of platform-driven markets.

43 European Commission, Shaping Europe's Digital Future, COM(2020) 67 final (19 February 2020).

5.3. Substantive Sustainability: Beyond Consent-Centric Regulation

Sustainable data protection requires recalibrating substantive legal standards beyond exclusive reliance on consent. As comparative analysis indicates, proportionality-based assessments, legitimate interest balancing, and risk-tiered obligations provide more robust safeguards against excessive data extraction and abusive profiling. Vietnam's PDPL currently lacks these substantive instruments, resulting in compliance strategies that prioritize formal disclosures over meaningful risk mitigation.

Introducing sustainability-oriented substantive standards – such as explicit limits on inferred data use, enhanced safeguards for automated decision-making, and clearer criteria for lawful profiling – would align consumer data governance with long-term fairness objectives rather than short-term transactional consent.

5.4. Sector-Specific Sustainability in E-Commerce Governance

E-commerce platforms present distinctive sustainability challenges due to continuous data generation, algorithmic personalization, and cross-platform integration. A sustainable regulatory framework should therefore incorporate sector-specific obligations tailored to these dynamics. Such measures may include standardized transparency dashboards, interoperable consent withdrawal mechanisms, and mandatory impact assessments for high-risk consumer data practices.

By embedding sustainability considerations into sectoral governance, regulators can address systemic risks at their source rather than relying on ex post enforcement. This approach also enhances regulatory predictability for businesses while improving consumer trust in digital marketplaces.

5.5. Sustainable Cross-Border Data Governance and Market Integration

Cross-border data flows are integral to the sustainability of Vietnam's e-commerce ecosystem. However, fragmented or opaque transfer rules may undermine both consumer protection and market integration. Comparative experience demonstrates that sustainable cross-border governance relies on interoperability mechanisms – such as adequacy assessments, mutual recognition frameworks, and standardized contractual safeguards – rather than rigid localization alone.

For Vietnam, developing sustainability-oriented cross-border data governance would support consumer protection while facilitating participation in regional and global digital trade regimes. Such alignment is essential for ensuring that data-driven growth remains compatible with long-term regulatory coherence and international trust.

Framing consumer data protection through a sustainability-oriented governance lens highlights the limitations of short-term, consent-centric regulatory strategies. For Vietnam, advancing sustainable consumer data protection entails integrating proportionality-based standards, diversified oversight mechanisms, and sector-specific safeguards into the implementation of the PDPL. This approach allows consumer data governance to evolve alongside digital market development, reinforcing long-term consumer trust and regulatory coherence.

6 Conclusion

This paper has examined consumer data protection in Vietnam's e-commerce sector through the lens of sustainability-oriented governance. Moving beyond a narrow focus on consent and procedural compliance, the analysis has demonstrated that data-intensive commercial ecosystems generate cumulative and systemic risks that require long-term regulatory responses. Conceptual distinctions between personal data and consumer data, coupled with an assessment of privacy, data protection, and consumer protection frameworks, reveal structural limitations in Vietnam's current regulatory approach.

Comparative analysis of the GDPR, China's PIPL, and the CCPA highlights that sustainable consumer data protection depends not solely on the recognition of individual rights, but on the integration of proportionality-based standards, diversified enforcement architectures, and sector-specific safeguards. These elements enable regulators to address profiling, inferred data use, and cross-border data flows more effectively than consent-centric models alone.

For Vietnam, adopting sustainable data protection as a governance principle provides a coherent pathway for refining the implementation of the PDPL without undermining its normative foundations. By embedding sustainability-oriented criteria – such as accountability, institutional coordination, and long-term market fairness – into consumer data regulation, Vietnam can better align digital economic growth with consumer trust and regulatory resilience. These insights underscore the importance of treating consumer data protection not as a static compliance obligation, but as an evolving governance project.

Bibliography

Ayunda Rahmi "Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties?" *Law Reform*, No. 2 (2022): 144-163. https://garuda.kemdikbud.go.id/documents/detail/3196813.

Bolatbekkyzy Gulbakyt, "Comparative Insights from the EU's GDPR and China's PIPL for Advancing Personal Data Protection Legislation" *Groningen Journal of International Law*, 11 (2024): 129-146. https://doi.org/10.21827/GroJIL.11.1.129-146.

Calzada Igor, "Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)" *Smart Cities*, No. 3 (2022): 1129-1150. https://doi.org/10.3390/smartcities5030057.

Casalini, Francesca, Javier López González, "Trade and Cross-Border Data Flows" *OECD Trade Policy Papers*, No. 220 (2019). https://doi.org/10.1787/b2023a47-en.

Cohen Julie E., *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford: Oxford University Press, 2019.

European University Institute. *Guide on Good Data Protection Practice in Research*. Florence: European University Institute, 2022. https://www.eui.eu/documents/servicesadmin/deanofstudies/researchethics/guide-data-protection-research.pdf.

Goel Archana, Utkal Khandelwal, Jayalakshmy Ramachandran, "Three Decades of Consumer Protection Literature: Systematic Review and Future Research Agenda" *Journal of Creative Communications* (2025), https://doi.org/10.1177/09732586251336493.

Greenleaf Graham, "Vietnam's 2024 Draft Data Privacy Law Is Ambitious and Ambiguous" *Privacy Laws & Business International Report*, 192 (2024): 22-25. https://doi.org/10.2139/ssrn.5124884.

Kuner Christopher, *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press, 2013.

Lam Tố Trang, "Some Legal Aspects of Personal Data Protection in the World – Experience for Vietnam" *Cogent Social Sciences*, No. 1 (2024). https://doi.org/10.1080/23311886.2024.2414872.

Mayer-Schönberger Viktor, Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Boston: Houghton Mifflin Harcourt, 2013.

Millard Christopher, W. Kuan Hon, "Defining 'Personal Data' in e-Social Science" *Information, Communication & Society*, 15 (2011). https://doi.org/10.2139/ssrn.1809182.

Morozov Evgeny, *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York: PublicAffairs, 2013.

OECD, "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value" *OECD Digital Economy Papers*, No. 220 (2013).

Phuong, Nguyen Duy. Nguyen Duy Thanh, "Law on Corporate Social Responsibility for Consumers in Vietnam" *Prawo i Więź*, No. 1 (2022): 297-312. https://doi.org/10.36128/priw.vi39.353.

Solove Daniel J., *Understanding Privacy*. Cambridge: Harvard University Press, 2008.

Solove Daniel J., Woodrow Hartzog, "The Scope and Potential of FTC Data Protection" *George Washington Law Review*, 83 (2015): 2230-2273.

Wagner Ben, *Algorithmic Regulation*. Oxford: Oxford University Press, 2022.

Zuboff Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.