Sarcouncil Journal of Public Administration and Management

ISSN(Online): 2945-3712

Volume- 05| Issue- 03| 2026

Research Article **Received:** 10-04-2026 | **Accepted:** 05-05-2026 | **Published:** 20-05-2026

Legal Framework for Personal Data Protection in E-Commerce in Vietnam in the Context of Digital Transformation

Nguyen Truc Thien

Nguyen Hoai Phuong

Abstract: In the context of the Fourth Industrial Revolution and the rapid advancement of digital transformation, e-commerce has become an integral component of Vietnam's digital economy, fundamentally reshaping business practices and consumer behavior. The widespread adoption of digital technologies such as big data, artificial intelligence, and digital platforms has enhanced business efficiency while significantly increasing the collection, processing, and exploitation of consumers' personal data. In the e-commerce environment, personal data not only includes basic identification information but also extends to behavioral data, transaction histories, financial information, and inferred data, generating substantial economic value for businesses. However, the digitalized nature and rapid dissemination of data have also intensified the risks of data misuse, infringements of privacy, and violations of personal data protection rights. In response to these challenges, although Vietnam's legal framework on personal data protection in e-commerce has been gradually developed, it still reveals certain limitations arising from the fact that legal regulations and enforcement practices have not fully kept pace with the rapid development of digital technologies and business models. This paper analyzes Vietnam's legal framework for personal data protection in e-commerce under the impact of digital transformation, employing a comparative legal approach with international standards. The study identifies key shortcomings in both regulatory provisions and law enforcement practices and proposes directions for legal improvement aimed at strengthening the protection of consumers' personal data rights, while ensuring an appropriate balance between safeguarding privacy and promoting the sustainable development of e-commerce in Vietnam.

Keywords: E-Commerce, Data Protection, Digital Transformation.

INTRODUCTION

In the face of international economic integration and a global digital transformation movement, e-commerce has become an important component of the digital economy. In Vietnam, widespread access and use of the Internet, smart devices, and digital platforms has allowed electronic shopping, payment, and transaction activities to grow in scale and forms. Revenue from e-commerce has consistently maintained high growth rates over the past many years, reflecting the growing role of this sector in the national economic structure and the process of shifting Vietnam's growth model to becoming one based on digital technology.

Along with the rapid development of e-commerce comes the collection, processing, storage, and extraction of an ever-increasing amount of personal data from consumers. In the digital environment, personal data is not just information for simple transactions but has become a type of "digital asset" with high economic value, playing a key role in building business strategies, personalizing services, analyzing consumer behavior, and enhancing the competitiveness of businesses. However, the characteristics of data – namely its digitalized, inter-connected, and rapidly disseminatable nature, increases the risks of misuse, leakage, privacy violations, and unauthorized exploitation, posing significant challenges to protecting the legitimate rights and interests of consumers in e-commerce.

Personal data in e-commerce is understood as all information associated with a specific individual. This data is collected, stored, processed, and extracted through electronic transactions on digital platforms for purposes such as transaction processing, consumer management, personalizing consumer experience, and market development. This represents a combination of the traditional approach to personal data with digital technology and modern commercial practices, reflecting the unique characteristics of online transaction during digital transformation.

In Vietnam, the legal framework for personal data protection has been gradually perfected over time, particularly with the dissemination of Decree No. 13/2023/ND-CP dated April 17, 2023 on personal data protection. This decree provides a definition for personal data as information in the form of symbols, writing, numbers, images, sounds, or similar forms associated with a specific individual or identifiable to that individual. The decree also stipulates the principles for processing personal data, the rights of the original owners of the data, and the responsibilities of agencies, organizations, and individuals involved in the collection, use, and processing of data. In the field of e-commerce,

***Corresponding Author:** Nguyen Truc Thien

DOI-https://doi.org/10.5281/zenodo.20315413

compliance with these regulations is especially important to ensure proper utilization of the economic value of personal data and the protection of the privacy and legitimate rights of consumers in the digital environment.

Personal data in e-commerce carries unique differences compared to personal data in the traditional sense. Firstly, e-commerce personal data is highly digitized, primarily existing in electronic form and processed through information technology systems. Secondly, the data is interconnected and is widely disseminated, easily shared, transferred, and extractable across various platforms, including internationally. Thirdly, e-commerce personal data has significant economic value due to its connection to data analysis, targeted advertising, and personalized services. Fourthly, the data is dynamic, constantly updated and changing over time, continuously reflecting changes in consumer behavior and needs. Finally, personal data in e-commerce can become a significant threat to privacy as without appropriate security measures and governance mechanisms, data can be illegally collected, leaked, bought and sold, or exploited for improper purposes.

The above characteristics show that protection of personal data in e-commerce in the context of **digital transformation** is an objective an essential need, not only for the protection of the legal rights and benefits of consumers but to reduce legal risks, and enhance the reputation and the sustainable development of businesses in the digital business environment. According to Article 3 of Government Decree No. 13/2023/ND-CP dated April 17, 2023, the protection of personal data in e-commerce must adhere to the following basic principles: the principle of legality and transparency; the principle of (serving a) specific purpose; the principle of minimizing collection of data; the principle of ensuring accuracy and timeliness; the principle of confidentiality during processing; the principle of retaining data only for the necessary period; the principle of accountability; and the principle of protecting the legitimate rights and interests of data subjects. These principles form an important legal foundation for building and implementing a mechanism for protecting personal data in e-commerce in Vietnam.

Therefore, there has been a constant push for the improvement of the legal framework around personal data protection through a system of relevant laws and sub-laws. Regulations around protecting privacy and personal data are reflected in the following laws: the Law on Consumer Rights Protection 2010 (amended and supplemented in 2023), the Law on Electronic Transactions 2005 and 2023, the Law on Information Technology 2006, the Law on Network Information Security 2015, along with Government Decree No. 52/2013/ND-CP dated May 16, 2013 on e-commerce and other relevant specialized decrees and circulars. Decree No. 13/2023/ND-CP on the protection of personal data in particular is a major step forward by establishing principles for data processing, the rights of original data owners, and the specific legal responsibilities of organizations and individuals involved in processing personal data in the digital environment.

The Vietnamese legal system has taken the first step towards establishing an important legal basis for protecting the privacy and personal data of consumers in e-commerce, while further highlighting the legal responsibility of e-commerce businesses in the collection, processing, storage, and security of personal data. This is a necessary prerequisite for building a safe and transparent electronic transaction environment and promoting consumer trust in the context of digital transformation.

However, the rapid digital transformation process, development of digital technology, and the requirements of international economic integration have exposed the current limitations of the legal system. Regulations on personal data protection in e-commerce are currently fragmented, lacking uniformity, while a specialized law on personal data protection has yet to be fully formed. Furthermore, some regulations have not kept pace with the development of new digital business models, cross-border digital platforms, and advanced data processing technologies, and have not fully met common international standards on personal data rights.

While the expansion of e-commerce in both scale and scope has increased the volume of personal data collected, processed, and extracted, current legal practice has given rise to many new and complex issues. In particular, challenges related to personal data breaches, difficulties in monitoring and handling violations, overlapping state management authority, as well as limited awareness and compliance with the law by both businesses and consumers, are becoming urgent issues in the current period.

Publisher: SARC Publisher

THE STATE OF APPLYING PERSONAL DATA PROTECTION LAWS IN E-COMMERCE IN VIETNAM

The State of Personal Data Protection in E-Commerce in Vietnam from 2023 – Now

Since 2023, digital transformation has flourished in most aspects of economy and society, maintaining rapid growth in terms of market scale, number of participants, and transaction value. Along with the fast expansion of e-commerce platforms and social media platforms integrating sales functions as well as digital payment methods, the collection, processing, and extraction of personal data is becoming more and more prevalent and systematic.

According to research reports and sociological surveys conducted by reputable domestic and international organizations, including a survey included in the Vietnam E-commerce Report 2023 by the Department of E-commerce and Digital Economy (Ministry of Industry and Trade) of approximately 11,000 individual consumers and 10,000 businesses, the level of participation of individuals and businesses in electronic transactions is gradually rising. Current Vietnamese law recognizes and protects the principle of legal validity of electronic transactions, stipulating that parties involved in a transaction cannot deny the legal validity, authenticity, and binding nature of the transaction simply because it was established electronically. This is an important legal foundation to ensure legal security for entities in the e-commerce environment and promote trust in digital transactions.

However, current practice of laws on personal data protection in e-commerce shows that the leakage, infringement, and illegal exploitation of consumers' personal data are still widespread and on the rise, leading to serious consequences. The leakage of personal data not only directly affects the privacy, financial security, and personal lives of consumers but also diminishes the reputation, brand, and competitiveness of businesses, while posing risks to cybersecurity and social order.

In reality, many personal data leaks originate from e-commerce platforms, payment intermediary services, consumer management systems, and digital applications related to online transactions. According to Viettel Threat Intelligence, over 61 million user accounts have had their data leaked recently, an increase of approximately 1.5 times compared to the same period in 2023. Sectors heavily affected include social media, banking, online transactions, education, and healthcare – areas with high levels of personal data collection and processing in the digital environment.

These figures show that, although the legal framework for personal data protection has created an important legal basis for personal data protection in e-commerce, especially with the dissemination of Decree No. 13/2023/ND-CP, the gap between legal regulations and practice remains quite large. Some e-commerce businesses have not taken compliance with personal data protection laws seriously enough. The mechanisms for inspection, monitoring, and handling violations still face many challenges, while consumers' legal awareness and data protection skills remain limited.

With the impact of digital transformation looming large, a reassessment of the effectiveness of applying personal data protection laws in e-commerce in Vietnam is now an urgent requirement. This will help identify why these violations happen, the shortcomings in enforcement mechanisms, and propose appropriate solutions to improve the effectiveness of personal data protection in the current e-commerce environment.

VIETNAMESE LAWS ON CONSUMER PERSONAL DATA PROTECTION IN E-COMMERCE

Legal basis

In Vietnam, the issue of personal data protection in general, and consumer personal data protection in e-commerce in particular, is currently governed by a multi-layered, multi-sectoral legal framework, with the most direct and central regulations being stipulated through legal documents below law level. Government Decree No. 13/2023/ND-CP dated April 17, 2023 on the protection of personal data is the first document to create a comprehensive legal framework on this matter, providing a definition of personal data, data processing principles, data subject rights, and the legal obligations and responsibilities of organizations and individuals involved in the collection, processing, and extraction of personal data in the digital environment, including e-commerce.

Although Decree No. 13/2023/ND-CP was a major leap forward in establishing a personal data protection mechanism in Vietnam, legally speaking, it is not yet a law and as such, does not

Publisher: SARC Publisher

have the same legal effect as laws enacted by the National Assembly. Therefore, the stability and legal binding nature of regulations on personal data protection, especially in the e-commerce sector directly and rapidly influenced by digital transformation, still have certain limitations. The lack of a specialized law on personal data protection means that the current legal system has not yet truly formed a long-term and unified legal foundation strong enough to comprehensively regulate the relationships within the modern e-commerce environment.

With this in mind, the Party and State have released guidelines that emphasized the need for increased protection of the legal rights of consumers, including protection of private data, while affirming the Party's role in building and implementing policies and laws on consumer protection in the digital economy. From this perspective comes an urgent need for the development and promulgation of a specialized law on personal data protection with a higher degree of legal validity, a clear scope of regulation, and long-term stability, in order to meet the rapidly developing demands of e-commerce under the impact of digital transformation.

The promulgation of the **Personal Data Protection Law** is necessary to fully and uniformly regulate fundamental aspects such as: the definition and classification of personal data; the scope of regulation and applicable subjects; the principles of data processing; the rights and obligations of data subjects, data controllers, and data processors; independent monitoring mechanisms; administrative, civil, and criminal punishments for violations when necessary; as well as specific regulations applicable to e-commerce and digital platforms. More importantly, this law needs to be designed to ensure legal stability while being able to adapt to the rapid changes in digital technology, avoiding obsolescence and delay in updating to the new status quo.

Besides Decree No. 13/2023/ND-CP, regulations on personal data protection in e-commerce are also included in laws such as the Cybersecurity Law of 2018, the Electronic Transactions Law of 2023, the Consumer Rights Protection Law of 2023, the Information Technology Law of 2006, and the Network Information Security Law of 2015. However, the dispersion of regulations on personal data across various legal documents has led to a lack of consistency and uniformity during implementation, especially in the field of e-commerce where complex and inter-sectoral legal relationships are rapidly arising.

In reality, this lack of uniformity is also shown through the division of authority in terms of state management and handling of violations related to personal data infringement in e-commerce. In many cases, agencies such as the Ministry of Public Security, the Ministry of Science and Technology, and the Ministry of Industry and Trade all have state management functions related to personal data, but there is no effective coordination mechanism or clear delegation of responsibilities between these agencies. This not only makes it difficult to handle incidents of personal data leaks and violations but also causes confusion among e-commerce businesses in identifying the management authority to fulfill their legal obligations.

The inconsistency and lack of uniformity in the current legal system have created "legal gaps" in personal data protection in e-commerce. In some cases, businesses may exploit legal ambiguities to collect, use, and share consumers' personal data beyond what is necessary or for improper purposes. On the other hand, consumers face difficulties in exercising and protecting their rights due to the lack of specific legal grounds and the competent authorities responsible for protecting their interests. This is among the core issues that needs to be analyzed and addressed to improve personal data protection laws in e-commerce in Vietnam within the context of digital transformation.

Rights of Individuals to Their Personal Data in E-Commerce

Current Vietnamese laws have taken the first steps in recognizing the basic rights of individuals to their personal data, including the rights to know, rights to consent, rights to access, rights to modify, remove, and restrict data processing. However, in e-commerce, ensuring that these rights are enforced and exercised still face many setbacks, unfitting of the rapid growth of the digital economy.

Firstly, the "rights to know" of the data subject refers to the rights to be fully, timely, and clearly informed of the purpose, scope, and type of personal data being gathered, as well as the processing method and relevant third parties, which has yet to be fully respected in the e-commerce environment. In reality, most e-

Publisher: SARC Publisher

commerce and other digital platforms only express these points through "privacy protection policies" or "terms of use" which are long and complicated, with heavy use of legal jargons, and is often placed on hard-to-reach places on websites or apps. Users are almost never given this information in an intuitive, easily understood manner before account registration or committing to a transaction, leading to the right to know being mostly performative in nature.

Similarly, although the "right to consent" in personal data collection and processing has been instated by law, in reality, this right is often stripped to a form of "consent by default". Consumers are forced to accept every single term to gain access to the service, without the right to individually choose which data processing purpose they give their consent to. This "combined" or "once for all" form of consent severely diminishes the value of voluntary, transparent, and informed consent, which is a cornerstone of personal data protection in the digital environment.

As for the rights to access, supplement, and modify personal data, consumers are also facing significant barriers. Most e-commerce platforms only allow users to modify basic information such as names, phone numbers, or delivery address, without allowing them full access to all the data that has been collected and processed. Other important data such as transaction history, consumer behaviour, consumer profiling, tracking data, cookies, or tracking technology are never published or remain unable to be accessed by even the data subjects themselves.

Many e-commerce platforms have no mechanism to allow users to request to modify or update sensitive or outdated personal data, leading to incorrect information still being stored and used in analysis, advertisement, or product recommendation. According to a report from the Ministry of Science and Technology in 2024, only around 24% of e-commerce platforms in Vietnam provide users with tools to relatively fully manage and modify their personal information, while a majority of platforms deny access to previously collected data or have no clear processes to exercise these rights.

In conclusion, it can be said that the rights of individuals to their personal data in e-commerce in Vietnam have only been recognized by letter of law but are yet to be fully protected in practice. Fundamental rights such as the right to know, right to consent, right to access, and right to modify are limited by the lack of a user-friendly interface, transparent data processing procedures, and especially the lack of a sufficiently severe punishment to force e-commerce platforms to fully comply. This is one of the greatest challenges in creating a safe, transparent, user-centered e-commerce environment in the context of digital transformation today.

State of Handling of Personal Data Infringement in E-Commerce.

Various limitations exist in how personal data protection infringement is currently handled, mostly due to the incompleteness and inconsistency of the legal framework regarding sanctions. Although Decree No. 13/2023/ND-CP has laid an important legal foundation for the protection of personal data, this document does not specifically stipulate a corresponding system of sanctions for each violation and generally puts it as "according to legal regulation". This forces authorities to instead apply the provisions of the Cybersecurity Law 2018, the Law on Consumer Rights Protection 2023, Decree 15/2020/ND-CP, or the Penal Code, and yet these documents are not designed to be consistent with the context of data handling in e-commerce.

As a result, the process of detecting, investigating, and punishing personal data infringement is often lengthy, inefficient, and fails to provide a deterrent for other would-be violations. According to statistics from the Information Security Department of the Ministry of Science and Technology, in 2023, more than 1,800 reports and complaints related to the leakage, collection, and unauthorized use of personal data were recorded, but only a fraction of them are ever properly handled and penalized. The large gap between the number of recorded violations and the number of cases processed shows that the current law enforcement mechanism is lacking and is still far behind the development of e-commerce and the digital economy.

Furthermore, current laws do not yet have a mechanism for classifying the severity of personal data breaches, leading to a rather "egalitarian" treatment of all violations. Minor violations, such as sending unauthorized advertisements, and particularly serious violations like large-scale theft and trafficking of personal data are not clearly defined in terms of legal responsibility and penalties. Current administrative fines, such as those stipulated in Decree 15/2020/ND-CP, are

Publisher: SARC Publisher

generally low compared to the economic benefits that violations in e-commerce can generate, thus failing to realistically deter future violations.

Furthermore, the mechanisms for protecting consumer rights after data breaches remain extremely limited. E-commerce platforms currently have virtually no clear legal obligation to compensate or assist consumers when personal data is leaked or misused, unless there is a separate agreement in their privacy policy. This makes it difficult for consumers to claim compensation or restore their data rights, undermining the protective role of the law in the digital environment.

A comparison with international standards reveals a significant gap in Vietnam's mechanisms for handling personal data breaches. Other legal models such as the European Union's GDPR or South Korea's data protection law clearly identify the relevant authority to impose penalties with severe fines being linked to generated revenue and establish mechanisms for legal action and compensation for individuals whose data has been violated. Meanwhile, in Vietnam, the lack of large-scale crackdowns and punishments serving as examples and effective civil litigation mechanisms has eroded public confidence in the ability of the law to protect their personal data, negatively impacting the sustainable development of e-commerce and the country's digital transformation process.

Controlling Mechanisms for Personal Data Protection in E-Commerce in Vietnam

Given the current pace of digital transformation, the mechanisms for controlling personal data protection in e-commerce in Vietnam still reveal many institutional and operational limitations, and other shortcomings in terms of practical competencies. At the local level, most specialized agencies, especially the Department of Science and Technology and other related units, have not been granted sufficient authority, human resources, and technological tools to monitor and inspect the collection, processing, and protection of personal data by e-commerce businesses in their areas. The process of receiving, classifying, and handling complaints from citizens regarding privacy violations remains largely manual, fragmented, and lacks standardized procedures.

The difficulties become even more apparent as the processing of personal data in e-commerce now increasingly stretches across localities and even countries. Many businesses use technology platforms, cloud computing, or servers physically located outside the current area, or even outside the territory of Vietnam, causing difficulties for local authorities in determining legal jurisdiction, collecting evidence, and applying appropriate measures. Furthermore, the staff responsible for personal data in many localities lack in-depth expertise in digital technology and data law, leading to delays in processing or the shifting of responsibility to the central level with an effective coordination mechanism yet to be in place.

At the central level, despite initial guidance and coordination from agencies such as the Ministry of Science and Technology and the Information Security Department, the inter-agency coordination mechanism between the Ministry of Industry and Trade (for e-commerce activities), the Ministry of Public Security (for cybersecurity and combating high-tech crimes), and the Ministry of Justice (for developing and reviewing legislation) remains overlapped, without clear delegation of responsibilities for each type of personal data breach. Thus, in practice, many cases show signs of personal data breaches but the agency primarily responsible for handling it cannot be identified, leading to prolonged investigation times, reduced effectiveness of handling, and weakened deterrence value.

Another systemic limitation is the lack of proactive control mechanisms and centralized oversight. Currently, information on personal data breaches largely relies on complaints from consumers or media coverage, rather than detection through technical monitoring tools and regular state inspections. Furthermore, Vietnam has yet to establish a unified monitoring database system to connect and share information across different levels and sectors. Meanwhile, personal data breaches in e-commerce are often interlinked, being organized by and involving multiple entities, requiring inter-sectoral control and comprehensive tracing capabilities.

Overall, the fragmentation in control mechanisms and the lack of effective cross-checking between different levels and sectors of the government, and between national and international digital spaces are ripping open significant "legal gaps" in personal data protection in Vietnam. This not only increases the risk of privacy violations for consumers in e-commerce but also erodes public trust in the effectiveness and efficiency of laws in the greater digital environment.

Publisher: SARC Publisher

Although Vietnam has made significant progress in establishing a legal foundation for privacy protection in recent times, particularly with the completion and promulgation of the legal framework for personal data protection, including the Personal Data Protection Law of 2025, challenges in enforcement remain substantial. Issues such as a lack of clear and sufficiently severe penalties, fragmented control mechanisms, and limited awareness and data protection skills on the side of the consumers are hindering the implementation of legal regulations in e-commerce in practice.

Therefore, the continuous improvement of control mechanisms for personal data protection toward enhancing intersectoral collaboration, investing into digital monitoring infrastructure, improving the capabilities of enforcing officers and promoting public awareness will be crucial. This not only ensures effective protection of the rights of consumers in the e-commerce space, but will serve as an important foundation for the sustainable, transparent, and reliable development of the e-commerce market in Vietnam in the age of digital transformation.

RECOMMENDATIONS FOR IMPROVEMENT

Improvement of the Legal Framework for Personal Data Protection in E-Commerce in Vietnam

Amidst the era of digital transformation and increasingly deep international economic integration, personal data protection in e-commerce has become an urgent legal requirement, closely linked to ensuring human rights, consumer rights, and the sustainable development of the digital economy. Although Vietnam has made significant progress in building a legal framework for e-commerce and personal data protection, the current legal system is still fragmented, lacking in uniformity and has not caught up to the rapid development of digital technology and platform-based business models. To improve the legal framework, the author suggests the following improvements:

Firstly, legal regulations related to e-commerce and personal data protection need to be reviewed, systemized, and synchronized. Current regulations are scattered across many documents at the law level and below, leading to overlaps and difficulties in application. Therefore, it is necessary to eliminate conflicting regulations, fill legal gaps, and improve the consistency and transparency of the legal system.

Secondly, regulations on personal data protection need to be specified in law, especially the core provisions currently regulated in Decree 13/2023/ND-CP to enhance the effectiveness, stability, and binding force of the law on e-commerce businesses. At the same time, related laws such as the Law on Electronic Transactions and the Law on Consumer Rights Protection need to be further amended and supplemented to be inclusive of new forms of digital transactions, online dispute resolution mechanisms, and the legal responsibilities of digital platforms in processing personal data.

Thirdly, any amendment to the legal system must ensure the inter-sectoral cooperation between e-commerce law and related laws such as civil law, commercial law, cybersecurity, competition law, tax law, and intellectual property law. This comprehensive approach helps to fully regulate the relationships born from e-commerce, avoiding legal fragmentation and minimizing risks in legal application.

Fourth, with the growth of cross-border e-commerce, legal harmonization and international cooperation has become essential. Selective adoption of international standards, especially the European Union's principles of personal data protection (GDPR), will help Vietnamese law better align with its international counterpart and protect the rights of consumers and businesses in cross-border digital transactions.

Fifth, the legal framework for personal data protection in e-commerce needs to be stable in principle but flexible in enforcement. The law should focus on stipulating fundamental principles, basic rights and obligations, while technical and more detailed points should be delegated to documents below the law level, which would allow for timely adjustments that can keep up with the development of digital technologies such as artificial intelligence, big data, and digital platforms. A clear mechanism for delegating responsibilities and coordination among state management agencies is needed, with a lead agency primarily responsible for personal data protection in e-commerce being specified alongside clearer coordinating roles of relevant ministries and sectors. This in turn would help overcome the current overlapping responsibilities

Publisher: SARC Publisher

and improve the effectiveness of inspection, supervision, and handling of violations.

Sixth, legal liability and sanctions for violations must be improved by increasing administrative monetary penalties for serious personal data breaches and expanding criminal liability in particularly serious cases. At the same time, the government should strengthen enforcement capacity of legal agencies, invest in digital monitoring infrastructure, and promote awareness campaigns to improve legal understanding among businesses and consumers.

In conclusion, the improvement of the legal framework of personal data protection in e-commerce is more than just making amendments to certain articles in isolation, but is the comprehensive renovation of the underlying institution, implementation, enforcement, and social awareness. This will serve as an important legal foundation to create a safe, transparent, and sustainable e-commerce environment in the era of digital transformation in Vietnam.

Strengthening of Personal Rights for Personal Data in E-Commerce

As e-commerce develops on the shoulders of the extraction of big data, the strengthening of personal rights regarding personal data should be identified as a central pillar of consumer protection law in the digital environment. Vietnamese law needs to fully recognize and specify the core rights of data subjects, including: the right to know, the right to consent or refuse, the right to withdraw consent, the right to access, edit, restrict processing, and delete data when the purpose of collection no longer exists. This approach is in line with modern legislative conventions, especially the GDPR, while ensuring a balance between privacy rights and digital business activities.

Besides recognizing these rights, the mechanism for enforcing personal data rights needs to be simple, transparent, and accessible in design. E-commerce platforms must be responsible for developing tools that allow consumers to directly manage their data on the system, instead of relying on formal privacy terms. Ensuring genuine user control is not only a legal obligation but also helps to consolidate trust and credibility for businesses in the digital environment.

To ensure personal data rights remain uncompromised, laws need to heighten the accountability and legal responsibilities of data processing businesses. These businesses must be able to prove their legality, transparency, and security in the entire data processing cycle and accept the strict penalties that come with violations, especially for misuse of data, failing to purge data, or allowing leakage to occur. Severe penalties would serve as the prerequisite to ensure that privacy rights are more than just on paper.

Digital technology should be seen as an essential support tool in the protection of personal data rights, deserving as much emphasis as making improvement to the law itself. Solutions such as data encryption, multi-factor authentication, artificial intelligence in detecting unusual access, or blockchain technology in tracing access requests can significantly enhance the ability to control and prevent data breach risks in e-commerce.

Lastly, the strengthening of personal rights must go hand in hand with raising social awareness. Consumers must be equipped with the legal and digital literacy to identify risks, take proactive measures to protect their information and effectively exercise their rights. Only through a combination of publicly available information, education, and guidelines can personal data rights be fully realized, contributing to a safe, transparent, and sustainable e-commerce environment in the era of digital transformation.

Stricter Handling of Personal Data Violations in E-Commerce

Firstly, the law needs to better clarify acts that would constitute violation of personal data in e-commerce. In practice, actions such as illegal extraction and selling of personal data, online scams, and exploiting e-commerce platforms to collect user information are yet to be included in existing regulations, causing difficulties in enforcement. Therefore, it is necessary to classify, list, and describe in great detail these violations, while constructing a flexible legal framework that would allow for timely adjustments as digital business models and the technology around it continue to change.

Secondly, it is necessary to increase the fines and diversify mechanisms for enforcement. Currently, the main tool of punishment is mainly administrative, with an amount severely disproportionate to the massive amounts of profits generated from personal data violation. Therefore, besides monetary fines, it is crucial that stricter punishments be introduced, such as suspension or withdrawal of business permits on e-commerce

Publisher: SARC Publisher

platforms, compensation for damages, publicizing of violations, and in even more serious cases, penal sentences for organized and large-scale acts of personal data violation.

Thirdly, the legal responsibility of subjects in the e-commerce environment must be clarified, especially that of e-commerce platforms and third-party service providers. The law needs to stipulate responsiblities in monitoring and controlling data, accountability, and joint liability when acts of personal data violation are committed on their platform. This is the key to elevating the social responsibility of businesses and enhancing the adminisrative efficiency of the government.

Fourth, modern digital technology such as AI or Big Data or Blockchain should be considered in monitoring and handling violations. This would help detect unusual activities in collecting and using personal data as quickly as possible. At the same time, the State needs to complete its digital information portals to receive complaints and reports from consumers, enhancing the transparency and enforcement efficiency of the law.

Besides making improvements to legal regulations, organization of enforcement should also be considered. The current state of enforcement has shown a lack of consistency between the application of the law in different localities which in turn leads to a reduction in its deterrence value. Therefore, it is necessary to improve the professional competencies of managing agencies, especially inter-sectoral inspectors in e-commerce, with emphasis on in-depth training and equipping them with modern tools in detecting and handling violations.

Lastly, the handling of violations in e-commerce need to go hand-in-hand with strengthening of international cooperation, given the rise in cross-border personal data violations. Cooperation with international agencies and organizations will help Vietnam improve its ability to prevent, investigate, and effectively deal with violations in the context of the global digital economy.

In conclusion, the creation of a just, transparent, and feasible enforcement mechanism would not only protect the rights of consumers and businesses, but create a firm legal foundation for the sustainable development of e-commerce in Vietnam in the era of digital transformation.

Specification of Controlling Mechanisms

Firstly, initiative must be given to local authorities such as the Departments of Industry and Trade, Public Security, Market Surveillance in managing, detecting, and handling violations related to e-commerce and personal data violation. However, to ensure objectivity and consistency, oversight from central governing bodies, such as the Ministry of Industry and Trade and the Vietnam E-commerce and Digital Economy Agency is required. These agencies need to conduct unplanned and planned inspections of their local counterparts, detecting and correcting mistakes during legal enforcement.

Secondly, horizontal and vertical cross-sectoral cooperation mechanisms should be established. These mechanisms would be used in especially serious, cross-province or cross-border crimes, requiring local authorities to report and work together with central authorities for consistent handling. Central authorities would also need to play a role in coordinating and providing professional guidance and technical support to prevent overlapping jurisdiction or passing-the-buck.

Thirdly, application of digital technology in monitoring and control will be crucial. It is necessary to create a national database for e-commerce syncronized from the central to the local level, allowing for information sharing and crosschecking in real time. Application of AI and Big Data will also help detect unusual behaviors and provide timely warnings against the selling of personal data, fraudulent transactions, or money laundering in the digital environment.

Fourth, the law would need to clearly stipulate the accountability of different levels of management within the cross-monitoring process. Central and local agencies must make periodic reports and take responsibility when serious violations within their jurisdiction occur. At the same time, strict punishments must be applied to acts of negligence, obstruction of justice or aiding illegal activities.

On the whole, cross-management mechanisms from the local to central level not only help improve the efficiency of detecting and handling violations in e-commerce, but create a foundation for a modern, transparent, and consistent administrative system. They would also provide a method for multi-dimensional information cross-checking, limiting risks of failure in detecting

Publisher: SARC Publisher

violations, while allowing the central government to make timely adjustments to policies.

Lastly, for this cross-management mechanism to operate effectively, investments into human resources and expansion of community involvement must be considered. E-commerce monitors must be trained in digital technology, international laws, and monitoring competencies in the digital environment; at the same time, professional associations, social organizations, and consumers must be encouraged to get involved, thereby forming a multilayered, multisubject controlling mechanism.

CONCLUSION

The widespread and rapid development of e-commerce within the greater picture of digital transformation has fundamentally changed methods of transaction, consumption, and data management in Vietnam. Within that process, personal data has become more than just a simple piece of identifiable information, but a highly valuable economic resource, closely associated with business models related to data, AI, and consumer behavior analysis. However, the increase in value and data extraction has led to greater risks of privacy breach, personal data exploitation, and a severe imbalance between the economic benefits that businesses stand to gain and basic rights of individuals.

The current state of e-commerce in Vietnam has shown that although the legal system around personal data protection in e-commerce has made significant strides, especially in the recognition of the rights of data subjects and the obligation of organizations in handling data, its effectiveness in practice is still limited. This might be due to a lack of consistency and overlap between legal regulations, as well as a significant gap between regulations and enforcement capacity, including ineffective monitoring mechanisms, insufficient penalties, as well as limitations in awareness and sense of responsibility among a certain number of businesses and consumers.

From a theoretical and practical perspective, it can be confirmed that personal data protection in e-commerce is more than just a technical issue, but a core part of digital economic administration and the protection of human rights in the digital environment. Improvements to legal regulations in this field would therefore need to be approached as a part of a comprehensive plan, rather than in isolation or passively reacting to violations as they happen. It needs to harmoniously combine statutory frameworks, an effective enforcement mechanism, application of modern technology, and the strengthening of international cooperation. In particular, benchmarking and selective localization of modern international conventions, such as the data protection model of the EU, will help Vietnam elevate its level of legal alignment and capacity for international integration

In the long run, personal data protection needs to be seen as a fundamental brick in building digital trust, ensuring the sustainable development of e-commerce and improving the competitive advantage of the economy. When personal data protection is ensured, businesses will be forced to adjust their business model towards transparency, responsibility, and respect for consumer privacy, while allowing the government to establish a stable and predictable legal environment, befitting of modern administrative requirements. This balance will generate a longlasting impetus for development, allowing Vietnamese e-commerce to grow not just in scale but in depth, becoming truly safe and sustainable in the digital era.

REFERENCES

1. Cao, T. “Cyberattacks in Vietnam are increasing rapidly. *Nhan Dan Newspaper*. (2024).
2. Duy, A. “Personal data of over 66% of Internet users illegally exploited in 2024.” *Vietnam Lawyers Journal*. (2024).
3. Protection, D. "General data protection regulation." *Intersoft Consulting, Accessed in October* 24.1 (2018).
4. Government of Vietnam. “Decree No. 52/2013/ND-CP on E-commerce. *Hanoi, Vietnam*. (2013).
5. Government of Vietnam. “Decree No. 85/2021/ND-CP amending and supplementing Decree No. 52/2013/ND-CP on E-commerce.” *Hanoi, Vietnam*. (2021).
6. Government of Vietnam. “Decree No. 13/2023/ND-CP on Personal Data Protection.” *Hanoi, Vietnam*. (2023).
7. Le, P. K. “Current situation and solutions for e-commerce development in Vietnam.” *Industry and Trade Magazine*, Vietnam. (2023).
8. National Assembly of Vietnam. “Law on Cybersecurity (No. 24/2018/QH14).” *Hanoi, Vietnam.* (2018).

Publisher: SARC Publisher

9. National Assembly of Vietnam. "Law on Protection of Consumers' Rights (No. 19/2023/QH15)." *Hanoi, Vietnam*. (2023).
10. National Assembly of Vietnam. "Law on Personal Data Protection." *Hanoi, Vietnam*. (2025).
11. Nguyen, G. T. "Current issues of personal data protection: International experience and recommendations for improving Vietnamese law." *Industry and Trade Magazine*, Vietnam. (2024).
12. Nguyen, T. N. T. "Legal framework and recommendations for improving the protection of consumers' personal data in e-commerce transactions." *Industry and Trade Magazine*, Vietnam. (2023).
13. Organisation for Economic Co-operation and Development (OECD). "The OECD Privacy Guidelines." *Paris: OECD Publishing*. (2013).
14. Solove, D. J. "Understanding Privacy." *Cambridge, MA: Harvard University Press*. (2021).
15. United Nations Conference on Trade and Development (UNCTAD). "Data Protection and Privacy Legislation Worldwide." Geneva: United Nations. (2021).
16. Vietnam E-commerce and Digital Economy Agency (iDEA), Ministry of Industry and Trade. "Vietnam E-commerce White Book 2023." *Hanoi: Industry and Trade Publishing House*. (2023).
17. Vietnam E-commerce and Digital Economy Agency (iDEA), Ministry of Industry and Trade. "Vietnam E-commerce White Book 2024." *Hanoi: Industry and Trade Publishing House*. (2024).
18. World Economic Forum. "Global Data Governance Framework: Shaping the Future of Data Economy." *Geneva: WEF*. (2022).

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Thien, N. T. "Legal Framework for Personal Data Protection in E-Commerce in Vietnam in the Context of Digital Transformation" *Sarcouncil Journal of Public Administration and Management* 5.3 (2026): pp 10-20.

Publisher: SARC Publisher