



## UUM JOURNAL OF LEGAL STUDIES

<https://e-journal.uum.edu.my/index.php/uumjls>

How to cite this article:

Tam, N. T. D., & Bang, N. T. K. (2026). Combating the illegal trading of personal data: Has Vietnam found the key to the puzzle? *UUM Journal of Legal Studies*, 17(2), 111-138. <https://doi.org/10.32890/uumjls2026.17.2.7>

### COMBATING THE ILLEGAL TRADING OF PERSONAL DATA: HAS VIETNAM FOUND THE KEY TO THE PUZZLE?

<sup>1</sup>Nguyen The Duc Tam & <sup>2</sup>Nguyen Thai Khanh Bang

<sup>1</sup>University of Economics and Law, Vietnam

<sup>2</sup>Vietnam National University, Vietnam

<sup>1</sup>Corresponding author: [tamntd@uel.edu.vn](mailto:tamntd@uel.edu.vn)

Received: 16/10/2024

Revised: 20/3/2026

Accepted: 31/3/2026

Published: 31/7/2026

#### ABSTRACT

In Vietnam, rapid digital transformation has fueled a growing demand for personal data across various sectors, much of which, unfortunately, is being met through illicit markets. This poses a serious threat to privacy and national cybersecurity. This paper analyzes the evolution and status of Vietnam's legal framework for personal data protection, assessing its effectiveness in curbing the illegal trading of personal data. To examine the issues at hand, this study employs the following methods: doctrinal analysis of relevant Vietnamese legal instruments; synthesis of secondary data from government reports, cybersecurity studies, and media sources; and a review of illustrative legal cases. The investigation has identified persistent legal and enforcement gaps, which included fragmented and sometimes inconsistent rules across instruments, an ineffective "notice-and-consent" model in practice, significant evidentiary barriers for victims, limited deterrence and operational enforceability of sanctions, and the absence of a tailored criminal offense targeting the illegal trading of personal data. Socio-psychological and technological drivers further incentivized breaches and undermined regulatory effectiveness. The paper proposes practical recommendations for Vietnamese lawmakers and regulators to strengthen enforcement mechanisms, harmonize domestic regulations, and promote public awareness and digital literacy. This paper offers a comprehensive assessment of Vietnam's evolving legal framework for personal data protection and provides practical guidance for policymakers in Vietnam and other developing jurisdictions seeking to curb the illegal trading of personal data and strengthen national data governance in the digital age.

**Keywords:** Cyber-routine activity theory, digital privacy, illegal trading of personal data, personal data protection, Vietnam.

## INTRODUCTION

The global digital transformation, accelerated by the COVID-19 pandemic, has led to unprecedented changes in how personal data is processed (Keck, 2021; The Economist, 2017). In Southeast Asia, since the adoption of the ASEAN Framework on Personal Data Protection (2016), the ASEAN Framework on Digital Data Governance (2018), and the ASEAN Data Management Framework (2021), ASEAN countries have faced an increasing need for stronger personal data protection frameworks (Rahman, 2025; Sholehuddin et al., 2024). Vietnam, as part of this global shift, has seen a growing demand for personal data across various sectors (VNS, 2023). In response, Vietnam designated 2023 as the National Year of Digital Data, underscoring the belief that personal data is a critical national resource and an invaluable input for the flourishing digital economy (VNA, 2023).

Recognizing the pivotal role of personal data in the digital era, Vietnam has revised and supplemented its relevant legal framework. As of 2025, although nearly 70 legal normative documents directly related to personal data have been enacted, the legal framework still lacks coherence in defining key concepts, including “personal data” and the scope of its protection (Chu, 2022). This inconsistency has hindered the effective safeguarding of personal data. In practice, the illegal trading of personal data remains a persistent issue in Vietnam. Cybercriminal activities related to personal data breaches show no signs of abating, posing a serious threat to individual privacy and cybersecurity (Anh, 2024).

This paper aims to support Vietnam’s long-term strategy to combat the illegal trading of personal data by strengthening the coherence and enforceability of its personal data protection framework. To achieve this aim, the study pursues the following four specific objectives: (1) to clarify and map key concepts and terminology across Vietnam’s relevant legal instruments, and in turn, highlighting key inconsistencies and regulatory fragmentation; (2) to document and analyze the current landscape of illegal trading of personal data in Vietnam by drawing on secondary reports and illustrative cases (2016–2025); (3) to evaluate the effectiveness of Vietnam’s existing civil, administrative, and criminal mechanisms in preventing, detecting, and sanctioning the illegal trading of personal data; and (4) to identify the main legal, socio-psychological, and technological drivers sustaining ongoing violations and as a result, propose targeted legal and policy reforms to strengthen Vietnam’s personal data protection regime. By integrating doctrinal analysis with secondary evidence, this study provides a timely assessment of Vietnam’s personal data protection regime and offers actionable reforms to curb the illegal trading of personal data.

Besides the Introduction, Methodology, and Conclusion sections, this paper is organized into four main parts. In Section 3, the authors examine the evolution and status of Vietnamese laws on personal data protection, with the view of highlighting inconsistencies within the legal framework. In Section 4, the authors analyze the current situation of illegal trading of personal data in Vietnam by discussing prevalent trends and notable cases. In Section 5, the authors explore the reasons behind personal data breaches, focusing on the legal, socio-psychological, and technological factors involved in personal data protection. In Section 6, the authors propose legal and policy solutions to combat the illegal trading of personal data, emphasizing harmonization with international standards, stronger enforcement, and public awareness efforts.

## METHODOLOGY

This study adopts a multi-method legal research design to assess Vietnam's capacity to prevent, detect, and sanction the illegal trading of personal data. It integrates (1) doctrinal legal analysis of the applicable normative framework, (2) documentary analysis of secondary reports on personal data breaches and illegal trading of personal data (2016–2025), and (3) jurisprudential analysis of publicly available Vietnamese court judgments.

First, the study thoroughly examines Vietnam's hierarchical legal framework governing privacy, personal information/data, and enforcement mechanisms to assess the scope, coherence, and effectiveness in addressing the illegal trading of personal data in Vietnam. The legal corpus comprises the Constitution, the Civil Code, sectoral laws, criminal law provisions, as well as administrative sanctioning decrees relevant to personal data protection. The legal instruments included in the corpus are listed in Table 1. Statutory interpretation is conducted with attention to Vietnam's hierarchy of norms and sectoral allocation of regulatory competence. Apparent normative inconsistencies are recorded as follows: (1) definitional inconsistency, (2) overlap or duplication, (3) legal gaps (unregulated situations), or (4) enforcement friction (rules that exist but are difficult to invoke in practice).

**Table 1**

### *Legal Instruments Included in the Legal Corpus*

| Document                                                                                                  | Type of document | Issuing authority | Legal status |
|-----------------------------------------------------------------------------------------------------------|------------------|-------------------|--------------|
| Before 2005                                                                                               |                  |                   |              |
| 1946 Constitution                                                                                         | Constitution     | National Assembly | Expired      |
| 1959 Constitution                                                                                         | Constitution     | National Assembly | Expired      |
| 1980 Constitution                                                                                         | Constitution     | National Assembly | Expired      |
| 1992 Constitution                                                                                         | Constitution     | National Assembly | Expired      |
| 1995 Civil Code                                                                                           | Code             | National Assembly | Expired      |
| Between 2005 and 2015                                                                                     |                  |                   |              |
| 2005 Civil Code                                                                                           | Code             | National Assembly | Expired      |
| 2005 Law on Pharmacy                                                                                      | Law              | National Assembly | Expired      |
| 2006 Law on Information Technology                                                                        | Law              | National Assembly | Expired      |
| Decree No. 64/2007/ND-CP on the Application of Information Technology in the State Agencies' Activities   | Decree           | Government        | Expired      |
| 2010 Law on Protection of Consumer Rights                                                                 | Law              | National Assembly | Expired      |
| 2013 Constitution                                                                                         | Constitution     | National Assembly | In force     |
| Decree No. 52/2013/ND-CP on E-commerce                                                                    | Decree           | Government        | Expired      |
| Decree No. 72/2013/ND-CP on the Management, Provision and Use of Internet Services and Online Information | Decree           | Government        | Expired      |

(continued)

| Document                                                                                                                                                                                       | Type of document | Issuing authority | Legal status      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|-------------------|-------------------|
| Between 2015 and 2023                                                                                                                                                                          |                  |                   |                   |
| 2015 Civil Code                                                                                                                                                                                | Code             | National Assembly | In force          |
| 2015 Criminal Code                                                                                                                                                                             | Code             | National Assembly | In force          |
| 2015 Law on Network Information Security                                                                                                                                                       | Law              | National Assembly | Expired           |
| 2016 Law on Children                                                                                                                                                                           | Law              | National Assembly | In force          |
| 2018 Law on Cybersecurity                                                                                                                                                                      | Law              | National Assembly | Expired           |
| Decree No. 15/2020/ND-CP on Sanctioning of Administrative Violations in the Fields of Postal Services, Telecommunications, Radio Frequency, Information Technology and Electronic Transactions | Decree           | Government        | Partially expired |
| Decree No. 98/2020/ND-CP on Sanctioning of Administrative Violations in Commercial Activities, Production of, Trading in Counterfeit or Banned Goods and Protection of Consumer Rights         | Decree           | Government        | Partially expired |
| Decree No. 117/2020/ND-CP on Sanctioning of Administrative Violations in Health Sector                                                                                                         | Decree           | Government        | Partially expired |
| Decree No. 119/2020/ND-CP on Sanctioning of Administrative Violations in Journalistic and Publishing Activities                                                                                | Decree           | Government        | Partially expired |
| Decree No. 38/2021/ND-CP on Sanctioning of Administrative Violations in Cultural and Advertising Sectors                                                                                       | Decree           | Government        | Partially expired |
| 2023 Law on Protection of Consumer Rights                                                                                                                                                      | Law              | National Assembly | In force          |
| Decree No. 13/2023/ND-CP on Personal Data Protection                                                                                                                                           | Decree           | Government        | Expired           |
| Between 2024 and 2025                                                                                                                                                                          |                  |                   |                   |
| 2025 Law on Personal Data Protection                                                                                                                                                           | Law              | National Assembly | In force          |
| 2025 Law on Cybersecurity                                                                                                                                                                      | Law              | National Assembly | In force          |
| Decree No. 356/2025/ND-CP on Detailing a Number of Articles and Measures for the Implementation of the Law on Personal Data Protection                                                         | Decree           | Government        | In force          |

*Notes.* Data was compiled by the authors from official Vietnamese legal documents.

Second, the study reviews secondary materials from 2016 to 2025 to characterize the operational landscape of illegal trading of personal data in Vietnam. Sources are prioritized as follows: (1) official legislative/policy materials connected to the development of the 2025 Law on Personal Data Protection (e.g., publicly available dossiers and explanatory submissions published on official portals of the National Assembly, Government, and Ministry of Public Security), (2) specialized cybersecurity reports that provide systematic summaries of personal data breaches (e.g., reports from Viettel Cyber Security, a subsidiary of Viettel Group), and (3) official media outlets reporting specific incidents (e.g., Nhan Dan, Public Security News, VietNamNet, VnExpress). Media reports are used primarily for illustration, and coverage of the same incident is cross-checked across multiple sources to reduce duplication and to verify factual accuracy.

Third, the study analyzes notable court and administrative cases related to personal data protection in Vietnam, including those adjudicated by Vietnamese courts and those handled by competent authorities. These court judgments are publicly available on the Supreme People's Court judgment portal. Given the limited number of published judgments directly centered on illegal trading of personal data, the study adopts an illustrative, purposive case-selection strategy to capture legally salient fact patterns. Each selected case is analyzed using a standardized extraction template, as follows: (1) factual pattern, (2) legal basis invoked, (3) evidentiary issues and burden of proof, (4) judicial reasoning and interpretation of key legal terms, and (5) outcomes and remedies/sanctions.

## **THE EVOLUTION AND STATUS OF VIETNAMESE LEGAL FRAMEWORK FOR PERSONAL DATA PROTECTION**

The formation and evolution of Vietnam's modern legal system since 1945 shows that an awareness of individual privacy rights was evident from the early days of the establishment of the Democratic Republic of Vietnam (now the Socialist Republic of Vietnam). Over the years, the concept of individual privacy has evolved to include rights related to personal and private secrecy. In this section, the authors examine key developments in the legal norms related to personal data protection in Vietnam, illustrating the perspectives of lawmakers through different stages.

### **The Constitution**

Since the first Constitution was promulgated in 1946, the modern Vietnamese law has always enshrined fundamental rights such as "the right to life, liberty, and the pursuit of happiness". However, due to wartime, the 1946 Constitution merely delineated these civil rights at a rudimentary level, without expansive applications across various domains. Notwithstanding this limitation, the 1946 Constitution did contain a specific provision, namely Article 11 pertaining to privacy rights concerning correspondence.

Subsequent 1959 and 1980 Constitutions expanded the scope of these rights, but retained inherent limitations. Specifically, Article 71 of the 1980 Constitution incorporated additional categories – "telephone and telegraph" – while ambiguously stating that "The secrecy of correspondence, telephones, and telegrams are guaranteed" without explaining what this assurance entailed.

In the 1992 Constitution, Article 73 more explicitly stipulated that "The safety and confidentiality of citizens' correspondence, telephones, and telegrams are ensured". Nevertheless, this provision did not delineate who is responsible for ensuring this safety and confidentiality.

Subsequently, the current 2013 Constitution clarified and perfected several provisions from the 1992 Constitution, introducing for the first time the term “personal privacy”. Article 21 of the 2013 Constitution widened the protective scope, stating that “Everyone has the right to inviolability of private life, personal privacy, and family secrecy; the right to protect one’s honor and reputation. Information regarding private life, personal privacy, and family secrecy is legally ensured for safety”. This provision introduced and provided the constitutional basis for the term “personal privacy”.

### **The Civil Code**

Although it was not until 2013 that the Constitution acknowledged the term “personal secrecy,” the Civil Code had previously referenced individual privacy rights. The first Civil Code in 1995 outlined “rights with respect to personal secrecy” in its Article 34, followed by provisions on “personal secrecy rights” in Article 38 of the 2005 Civil Code and continuing in Article 38 of the 2015 Civil Code, which further defined “rights to private life, personal secrecy, and family secrecy.”

An evident distinction between the 1995 and 2005 Civil Codes pertains to the title of the provision. While the 1995 version used the term “rights with respect to personal secrecy”, the 2005 version omitted the phrase “with respect to.” Both versions broadly stated that personal privacy “is respected and protected by law.” Nevertheless, Article 38 of the 2005 Civil Code modified the subjects who could consent to the collection and publication of information and materials on the private life of an individual in cases where the individual had died, lacked civil capacity, or was under 15 years old; extending this privilege to legally designated representatives beyond immediate family members.

The current 2015 Civil Code has declared “rights to private life, personal secrecy, and family secrecy” as “inviolable,” aligning with the principles of the 2013 Constitution. This change in the legal term reflects a more specific scope of legal protection, acknowledging that everyone, as an independent person under civil law, has a private life that contains personal secrets, including those shared among family members. However, the lack of a specific definition for these terms means that accurately determining the extent of legal protection remains challenging. Additionally, the 2015 Civil Code has expanded its scope to include “collection, storage, use, and publication of information,” where “storage and use” are activities newly added compared to the 1995 and 2005 Civil Codes, which only governed “collection and publication of information and materials.”

### **Other Laws and Regulations between 2005 and 2014**

Following the provisions of the 2005 Civil Code, other laws began addressing rights and obligations related to personal information. Noteworthy, the 2005 Law on Pharmacy introduced the term “personal information” (Article 57), albeit without a comprehensive definition. Furthermore, the 2006 Law on Information Technology included specific provisions on the collection, processing, and use of personal information on the Internet (Article 21), as well as the storage and provision of personal information on the Internet (Article 22); however, it too lacked a definitive explanation of “personal information”.

The Decree No. 64/2007/ND-CP on the Application of Information Technology in the State Agencies’ Activities was the first regulation to offer a general concept of “personal information,” defining it as “information sufficient to accurately identify an individual” (Article 3(5)). Later, the Decree No. 52/2013/ND-CP on E-commerce offered another perspective, defining it as “information that helps to identify an individual (...) and other information that the individual wishes to keep confidential” (Article 3(13)). Personal information does not include work contact information and information that

the individual has self-published in the media. Nevertheless, Decree No. 72/2013/ND-CP on the Management, Provision and Use of Internet Services and Online Information took an opposite approach, defining it as “information associated with the identification of individuals” (Article 3(16)), regardless of whether this information has been published. In short, between 2005 and 2014, legal provisions on the protection of personal information appeared across various legal texts without a consistent approach to the use and interpretation of legal terms. Notably, the term “personal information” had at least three divergent interpretations in different regulations, as presented in the foregoing discussion, leading to significant challenges in the application of the laws and regulations.

### **Other Laws and Regulations between 2015 and 2023**

The 2015 Law on Network Information Security, although not employing the same terminology as the 2015 Civil Code, has defined “personal information” as “information associated with identifying a specific individual” (Article 3(15)). It further introduces the term “subject of personal information” as “an individual identified through the personal information” (Article 3(16)). Moreover, the 2015 Law on Network Information Security has explicated “personal information processing” as “performing one or multiple operations of collecting, editing, using, storing, providing, sharing, and disseminating personal information online for commercial purposes” (Article 3(16)). Therefore, activities such as “collection, storage, usage, and publication” as regulated in the 2015 Civil Code are indeed forms of personal information processing.

The 2015 Law on Network Information Security explicitly prohibits activities such as “illegally collecting, using, disseminating, or trading in personal information of others; abusing weaknesses in information systems to collect or exploit personal information” (Article 7(5)). However, the scope of the 2015 Law on Network Information Security is primarily focused on network information security (Article 1), so this provision is insufficient to comprehensively prevent and combat the illegal trading of personal data. Furthermore, the 2015 Law on Network Information Security leaves unresolved issues concerning non-commercial personal data processing (Article 16(5)).

Within the cyber realm, the 2018 Law on Cybersecurity stipulates measures for ensuring societal security online and outlines responsibilities for relevant agencies, organizations, and individuals (Article 1). The 2018 Law on Cybersecurity was the first legislation to require online service providers to notify users in the event or potential occurrence of incidents involving leaks, losses, or damages to user data (Article 41(1)(c)). However, its provisions on user information security are only fundamentally principled in nature.

Children enjoy special protection with respect to their personal information since they are considered vulnerable. The 2016 Law on Children explicitly prohibits activities such as “announcing or disclosing information about the privacy or secret of the child without the consent of the child who is enough seven years old or older, or the consent of the child’s parent or guardian” (Article 6(11)). It further includes a provision devoted to preserving the children’s right to privacy, which reads:

#### **Article 21. Right to privacy**

1. Children have the imprescriptible right to privacy and keep personal and family secrets; all are for the best interests of children.

2. Children have their honor, dignity, personal prestige, mail, telephone and telegram security and other personal information exchange types protected by the law. They are protected from and may resist illegal interventions against personal information.

Moreover, child protective service providers must maintain confidentiality of information concerning abused children (Article 58(1)(dd)). The 2018 Law on Cybersecurity further safeguards the children by incorporating a specific provision for children protection in cyberspace (Article 29).

Another significant stakeholder group – consumers – also receives special attention. The 2010 Law on Protection of Consumer Rights includes a provision dedicated to the protection of consumer information (Article 6). The 2023 Law on Protection of Consumer Rights has introduced and elaborated on the concept of “consumer information,” which includes “personal information of consumers, information about the purchase and use of products, goods and services by consumers, and other information related to transactions between consumers and business organizations and individuals” (Article 3(3)). Moreover, the number of provisions related to consumer information in the 2023 version has increased sixfold compared to the 2010 version. These provisions include the following: (1) the protection of consumer information, (2) the formulation of rules on the protection of consumer information, (3) notification upon the collection and use of consumer information, (4) the use of consumer information, (5) the assurance of safety and security for consumer information, and (6) the checking, editing, updating, destruction, transfer, and discontinuation of the transfer of consumer information (Articles 15–20).

### **The 2023 Decree on Personal Data Protection**

On 17 April 2023, Decree No. 13/2023/ND-CP on Personal Data Protection (the 2023 Decree on Personal Data Protection) was issued, establishing a more comprehensive legal framework for personal data protection. It defines key terminology, outlines principles for personal data protection, and enumerates prohibited actions related to personal data, thereby laying the groundwork for the application of specialized legal regulations.

Unlike the term “personal information,” which had sporadically appeared in previous legal documents, the term “personal data” was officially defined for the first time in the 2023 Decree on Personal Data Protection. According to this decree, “personal data” refers to “information in the form of signs, writing, numbers, images, sounds, or similar forms in the electronic environment that is associated with a specific individual or facilitates the identification of a specific individual. Personal data encompasses both basic and sensitive personal data” (Article 2(1)). There is a perspective that, from the standpoint of information security – which involves protecting information and information systems to ensure integrity, confidentiality, and availability – the concepts of “information” and “data” are essentially indistinguishable (Quynh, 2020). Consequently, some Vietnamese scholars view regulations on “personal information” as also applying to “personal data,” given the closeness of these two concepts. However, under the 2023 Decree on Personal Data Protection, “personal data” is defined as “information (...) in the electronic environment,” which distinguishes it from “personal information.” The latter has a broader implication as it includes non-electronic information as well.

The 2013 Constitution states that “human rights and citizens’ rights can only be restricted as prescribed by law and only when necessary for national defense, security, social order, morality, or community well-being” (Article 14(2)). Despite this, the 2023 Decree on Personal Data Protection outlines specific instances where personal data may be processed without the individual’s consent (Articles 17 and 18).

The Government contends that incorporating these exceptions into the decree – though merely a regulatory instrument and not a law – is essential for its effective enforcement. Omitting such provisions would severely disrupt current personal data processing activities. While drafting the decree, the Government conveyed these concerns to the National Assembly in Report No. 442/BC-CP, dated 1 October 2020. In the report, the Government advocated for the continued development of the decree and expressed its intention to formulate a comprehensive draft Law on Personal Data Protection in the future.

Although previous laws have addressed the principles and regulations for protecting personal information to some extent, the 2023 Decree on Personal Data Protection is the first legal document to explicitly prohibit the trading of personal data in all forms (Articles 3(4) and 22(2)). However, because this decree has lower legal authority compared to laws, the latter must still be applied first when handling cases related to personal data protection. Therefore, the provisions regarding the principles of personal data protection (Article 3) and the rights of data subjects (Article 9) in this decree typically include the exception “unless otherwise provided by law.”

### **The 2025 Law on Personal Data Protection and the 2025 Law on Cybersecurity**

On 26 June 2025, the National Assembly adopted the 2025 Law on Personal Data Protection (Law No. 91/2025/QH15). This law comprises 39 articles in five chapters, governs personal data, personal data protection, and the rights, obligations, and responsibilities of relevant agencies, organizations, and individuals (Article 1(1)). Having taken effect on 1 January 2026, it is the first statute in Vietnam to regulate personal data and personal data protection in a specialized and comprehensive manner.

The 2025 Law on Personal Data Protection defines “personal data” as “digital data or information in other forms that identifies or helps identify a specific person” (Article 2(1)). Compared with the 2023 Decree on Personal Data Protection, this statutory definition is more general. At the same time, the 2025 Law on Personal Data Protection introduces an important clarification by providing that personal data, once de-identified, no longer constitutes personal data (Article 2(1)). This is a notable development because it gives the legal framework a clearer boundary. In a similar vein, the 2025 Law on Personal Data Protection defines “basic personal data” and “sensitive personal data” in broader terms and leaves the detailed listing of these categories to the Government (Articles 2(2) and 2(3)). This legislative technique appears intended to preserve flexibility and allow subsequent adjustment in light of changing technological and regulatory conditions. Decree No. 356/2025/ND-CP, which took effect on 1 January 2026, was issued to provide such implementation details.

The 2025 Law on Personal Data Protection also refines the legal treatment of the illegal trading of personal data. Unlike the 2023 Decree on Personal Data Protection, which addressed the illegal trading of personal data under the principles of personal data protection (Article 3(4)), the 2025 Law on Personal Data Protection places this matter directly among the prohibited acts (Article 7(6)). The law also provides greater clarity on several forms of data transfers that should not be treated as the trading of personal data, namely the following: (1) transferring personal data with the consent of the personal data subject; (2) sharing personal data between units of the same agency or organization to process personal data in conformity with the established processing purposes; (3) transferring personal data for further processing in the event of reorganization or termination of operation; (4) transferring personal data to the personal data processor or a third party for processing according to regulations; (5) transferring personal data at the request of a competent state agency; and (6) transferring personal data in cases of authorized non-consensual processing (Article 17(1)).

This clarification is significant because it narrows the ambiguity that existed under the 2023 Decree on Personal Data Protection and helps distinguish illegal trading of personal data from legally structured data transfers.

In addition, the 2025 Law on Personal Data Protection strengthens the protection of vulnerable data subjects such as children, persons with lost or limited civil act capacity, and persons with difficulties in cognition or behavioral control (Article 24) and expands sector-specific rules (Articles 25–32). Notably, among these sector-specific rules, the law expressly requires notification to data subjects in cases involving the leakage or loss of information on bank accounts, finance and credit, or credit information (Article 27(1)(d)).

The 2025 Law on Personal Data Protection is not merely declaratory; rather, it introduces a more operational framework for accountability, documentation, and regulatory supervision, moving Vietnam's legal framework for personal data protection toward a more structured compliance model.

A further legislative development occurred on 10 December 2025, when the National Assembly adopted the 2025 Law on Cybersecurity (Law No. 116/2025/QH15). This cybersecurity law took effect on 1 July 2026. It repeals both the 2015 Law on Network Information Security and the 2018 Law on Cybersecurity, thereby consolidating Vietnam's cyber-regulatory framework into a single statute. In this respect, the 2025 Law on Cybersecurity should be understood as an important structural reorganization of the legal architecture governing cyberspace.

The 2025 Law on Cybersecurity articulates more clearly several cyber-related acts that overlap with the illegal trading of personal data. Specifically, it prohibits, *inter alia*, the act of appropriating, trading, seizing, or intentionally disclosing personal secrets, family secrets, and privacy in a manner that affects the honor, reputation, dignity, rights, and legitimate interests of authorities, organizations, or individuals (Article 7(2)(c)) and the act of illegally collecting, using, disseminating, exchanging, transferring, or trading in personal information and data of others (Article 7(2)(h)). The 2025 Law on Cybersecurity provides a more explicit cyber-regulatory basis for addressing personal data-related misconduct, including conduct closely associated with the illegal trading of personal data.

Taken together, these two statutes mark a major turning point in the evolution of Vietnamese law in this matter of cybersecurity. If the 2023 Decree on Personal Data Protection represented the first comprehensive regulatory attempt to govern personal data, the 2025 Law on Personal Data Protection elevates that framework to the statutory level and adds greater conceptual clarity, broader sectoral coverage, and more structured compliance obligations. The 2025 Law on Cybersecurity, in turn, reinforces the cyber-enforcement dimension by consolidating earlier legislation and more expressly targeting unlawful acts involving personal data in cyberspace. As a result, Vietnam's legal framework on personal data has moved from a fragmented and terminologically inconsistent structure toward a more coherent multi-layer structure, consisting of a specialized statute on personal data protection and a broader statute on cybersecurity that supports enforcement against cyber-enabled violations, including the illegal trading of personal data.

### **Legal Remedies**

According to the current provisions in Vietnamese law, persons who engage in the illegal trading of personal data may be subject to (1) civil liability, (2) administrative fines, and (3) criminal responsibility.

First, civil liability for invasion of privacy encompasses both contractual liability and extracontractual liability (or torts). Under the 2015 Civil Code, parties to a contract may not disclose information about each other's private lives, personal secrets, and family secrets that they have learned during the formation and performance of their contract, unless otherwise agreed upon (Article 38(4)). Additionally, a person who violates another's honor, dignity, or reputation and thereby, causes harm must pay compensation, unless otherwise prescribed by the 2015 Civil Code or other relevant laws (Article 584(1)). Damages resulting from such violations include the following consequences: (1) reasonable expenses for limiting and remedying the damage, (2) lost or reduced actual income, and (3) other damages as prescribed by law (Article 592(1)). A person responsible for compensating for an infringement upon another's honor, dignity, or reputation must also pay an amount for the emotional distress caused to the victim. The amount of compensation for emotional distress should be agreed upon by the parties; if they cannot reach an agreement, the maximum compensation per victim is set at ten times the base salary as determined by the State (Article 592(2)).

Second, administrative penalties for violations involving personal information are stipulated across various sector-specific decrees, among which the following five documents are notable: (1) Decree No. 15/2020/ND-CP on Sanctioning of Administrative Violations in the Fields of Postal Services, Telecommunications, Radio Frequency, Information Technology and Electronic Transactions (as amended), (2) Decree No. 98/2020/ND-CP on Sanctioning of Administrative Violations in Commercial Activities, Production of, Trading in Counterfeit or Banned Goods and Protection of Consumer Rights (as amended), (3) Decree No. 117/2020/ND-CP on Sanctioning of Administrative Violations in Health Sector (as amended), (4) Decree No. 119/2020/ND-CP on Sanctioning of Administrative Violations in Journalistic and Publishing Activities (as amended), and (5) Decree No. 38/2021/ND-CP on Sanctioning of Administrative Violations in Cultural and Advertising Sectors (as amended).

Notably, Decree No. 15/2020/ND-CP (as amended) stipulates monetary fines ranging from 10,000,000 VND to 20,000,000 VND for providing personal information to third parties after the data subject has requested discontinuation of such provision (Article 84(1)). Furthermore, fines ranging from 40,000,000 VND to 60,000,000 VND are imposed for any of the following acts: (1) providing, sharing, or disseminating personal information that has been collected, accessed, or controlled to third parties without the consent of the data subject, and (2) illegally collecting, using, disseminating, or trading personal information of others (Article 84(2)). Additionally, this decree mandates the deletion of personal information obtained through these violations as a remedial measure (Article 84(3)).

Decree No. 15/2020/ND-CP (as amended) stipulates monetary fines ranging from 50,000,000 VND to 70,000,000 VND for the illegal trading or exchanging of private information of telecommunications service users (Article 102(5)(a)). An additional penalty is the revocation of the license to establish a social network for a period of 22 to 24 months (Article 102(8)(a)). Moreover, this decree requires the forcible restitution of any illicit gains obtained from committing these violations (Article 102(9)(a)).

In the field of e-commerce, Decree No. 98/2020/ND-CP (as amended) imposes monetary fines ranging from 30,000,000 VND to 40,000,000 VND for stealing, disclosing, transferring, selling information related to the trade secrets of other merchants or organizations, or the personal information of consumers, without the consent of the relevant parties (Article 63(5)(b)). Additional penalties include these measures: (1) the confiscation of objects and means used to commit the violation, and (2) the suspension of e-commerce activities for a period of six to twelve months (Article 63(7)). Remedial measures include these actions: (1) the compulsory retrieval of the ".vn" domain of the e-commerce

website or the removal of mobile applications from application stores or on provided addresses, and (2) the forcible restitution of any illicit gains obtained from committing these violations (Article 63(8)).

Besides these sector-specific decrees, the 2025 Law on Personal Data Protection introduces a much more stringent administrative penalty regime for the illegal trading of personal data. Under Article 8(3), the maximum monetary fine for the illegal trading of personal data is ten times the profit derived from the violation. Where no profit is obtained, or where the fine calculated on the basis of illicit profit is lower than the statutory ceiling, Article 8(5) provides for a maximum monetary fine of VND 3 billion. In comparison with the above-mentioned decrees, the 2025 Law on Personal Data Protection marks a significant increase in the severity of administrative sanctions, as the new statutory ceiling is more than 40 times higher than the highest monetary fine of VND 70 million prescribed under Decree No. 15/2020/ND-CP (as amended) for relevant acts involving the illegal trading of personal data. This development reflects a clear legislative shift from a fragmented, sector-based sanctioning model toward a more centralized and considerably stricter framework for addressing the illegal trading of personal data.

Third, the 2015 Criminal Code (as amended) does not specify a separate crime for the illicit use of personal data, but it includes two related offenses. The first is “Violation of the secrecy or security of correspondence, telephone calls, telegrams, or other forms of private communication” (Article 159), with a maximum penalty of three years in prison. Additionally, offenders may be fined from 5,000,000 VND to 20,000,000 VND and prohibited from holding certain positions for one to five years. The second offense is “Illegal transmission or use of information on computer networks or telecommunications networks” (Article 288), notably involving “the trading, exchanging, donating, modifying, changing, or publicizing of legal private information of agencies, organizations, or individuals on computer networks or telecommunications networks without the owner’s permission,” with a maximum penalty of seven years in prison. Offenders can also be fined from 20,000,000 VND to 200,000,000 VND and prohibited from holding certain positions or practicing certain professions for one to five years.

## **THE CURRENT SITUATION OF ILLEGAL TRADING OF PERSONAL DATA IN VIETNAM**

### **The Prevalence of Personal Data Breaches**

As of early 2024, Vietnam has 78.44 million Internet users, representing 79.1% of its population. About 72.70 million Vietnamese use social media, accounting for 73.3% of the population (Kemp, 2024). These figures highlight the vast scale of electronic personal data in Vietnam, as most Internet and social media users must provide personal information to access online services. This data is constantly at risk of unauthorized collection and use. Due to the nature of digital data, just one act of uploading and sharing a link or file can spread it globally via the Internet, creating countless copies. These copies can be downloaded and potentially sold on the black market (Quy, 2023).

Between 2016 and 2018, several incidents of customer data breaches occurred at major Vietnamese companies, notably including a hacker attack on Vietnam Airlines’ information system in 2016, which exposed the information of 411,000 VIP customers under the Lotuses membership program (Nam, 2016). In 2018, VNG (VinaGame) leaked over 163 million customer accounts (Son, 2018).

In 2019, the Ministry of Public Security identified over 60 organizations and individuals involved in the illegal trading and use of personal information in cyberspace (Le, 2021). Such data was repeatedly bought and sold. Data packages for sale covered various sectors such as employee lists, internal directories, Internet subscriptions, bank accounts, business registrations, information about students, teachers, and parents, real estate transactions, and selectively chosen personnel, along with customer lists of Internet services. These data types were traded over long periods, sometimes with accuracy guarantees and support for custom data extraction as per buyer requests (Quy, 2024).

According to the Ministry of Public Security, the illegal trading of personal data was conducted in two main ways (Le, 2021; Huong, 2020). First, companies that collected customer data allowed third parties to access it without stringent regulations, enabling these third parties to transfer and trade the information with others. Second, companies actively collected personal data to form databases, which they analyzed and processed for business purposes.

Between 2019 and 2020, the Ministry of Public Security discovered hundreds of individuals and organizations involved in the illegal trading of personal data, affecting millions of people with nearly 1,300 GB of personal data being illegally collected and sold (The Saigon Times, 2023). The illegal trading of personal data was not just an individual endeavor, but involved companies and organizations, with some companies investing in building and operating systems specifically designed for the illicit collection of personal data for profit (Anh, 2024). These systems include software that secretly gathers, compiles, and analyzes personal data from websites. The software also has malware designed to steal personal data from computers and mobile devices (VNS, 2024). There has been organized attacks to hijack personal data from the information systems of institutions and businesses.

In 2022, the Vietnam Information Security Association (VNISA) conducted a survey involving 135 businesses and organizations in Vietnam (VNISA, 2022). The results revealed that 76% of these entities did not have sufficient information security personnel to meet current requirements. Concerns were high among respondents, with 87% worried about human-related issues, 58% about technological factors, and 47% about procedural vulnerabilities. Moreover, 68% of the organizations lacked the necessary funding to invest in information security to meet their needs. The Authority of Information Security under the Ministry of Information and Communications assessed that 80% of personal information leaks are due to user negligence, providing opportunities for malicious actors to gather personal information for exploitation. The remaining 20% of leaks are attributed to service providers and typically involve vulnerabilities in their systems and applications, as well as gaps in their customer information security policies. Some of these businesses intentionally share customer data with third parties (NK, 2022).

From 2022 onward, Viettel Cyber Security's reports on the situation regarding information security risks in Vietnam have documented the following notable personal data breaches: 30 incidents in 2022 (Table 2), 40 in 2023 (Table 3), 108 in 2024 (Table 4), and 627 in 2025 (Table 5).

**Table 2**

*Notable Personal Data Breaches in Vietnam in 2022*

| Sector               | Number of incidents | Types of data exposed                       | Amount of data exposed          |
|----------------------|---------------------|---------------------------------------------|---------------------------------|
| Technology, Business | 4                   | System source code, customer data           | 2 TB of data, 5 million records |
| Education            | 3                   | Student information                         | 30 million records              |
| Retail               | 1                   | Customer data                               | 300,000 records                 |
| Finance              | 2                   | Customer data                               | 5 million records               |
| Other                | 20                  | Personal information, social media accounts | 100 million records             |

*Notes.* The source is Viettel Cyber Security (2023).

**Table 3**

*Notable Personal Data Breaches in Vietnam in 2023*

| Sector               | Number of incidents | Types of data exposed                                               | Amount of data exposed                                                               |
|----------------------|---------------------|---------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Retail               | 23                  | Source code of various retail media units                           | 3.5 million records<br>40,000 records                                                |
| Education            | 4                   | Information from major universities in Vietnam                      | 500 MB of database                                                                   |
| Technology, Business | 4                   | System source code, customer data                                   | 300 GB of source code                                                                |
| Manufacturing        | 3                   | Customer information from major manufacturing groups                | 1.8 million records<br>255,770 records                                               |
| Transportation       | 1                   | Customer information from a major transportation company in Vietnam | 1.5 million records                                                                  |
| Energy               | 1                   | System source code, customer data                                   | n/a                                                                                  |
| Aviation             | 1                   | Personal information, eKYC information                              | 90 million records                                                                   |
| Other                | 3                   | Personal information, eKYC information                              | 15 GB of source code,<br>3.9 million records<br>2.7 million records<br>4,000 records |

*Notes.* The source is Viettel Cyber Security (2024).

**Table 4**

*Notable Personal Data Breaches in Vietnam in 2024*

| Sector         | Number of incidents | Types of data exposed                                                                           | Amount of data exposed                                        |
|----------------|---------------------|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Technology     | 9                   | System source code, customer data                                                               | 121 million records<br>10 GB of source code<br>893 MB of data |
| Education      | 8                   | Personal information, documents of several universities and educational institutions in Vietnam | 17.3 GB of data<br>16 thousand documents<br>2 million records |
| Retail         | 51                  | Customer information, transaction information                                                   | 29 million records<br>55 KB of data                           |
| Transportation | 3                   | System source code, customer data                                                               | 2.3 GB of source code<br>6.5 million records                  |
| Aviation       | 2                   | Sensitive documents, customer data                                                              | 500 thousand records                                          |
| Finance        | 5                   | Customer information, data extracted from the internal system                                   | 13 million records                                            |
| Other          | 30                  | Personal information, eKYC information                                                          | 84 million records<br>137 GB of data                          |

*Notes.* The source is Viettel Cyber Security (2024, 2025).

**Table 5**

*Notable Personal Data Breaches in Vietnam in 2025*

| Sector                           | Number of incidents | Types of data exposed                        | Proportion of total exposed data (%) |
|----------------------------------|---------------------|----------------------------------------------|--------------------------------------|
| Consumer Services – Individuals  | 139                 |                                              | 75.36%                               |
| Finance – Banking                | 49                  |                                              | 6.25%                                |
| Insurance                        | 27                  |                                              | 5.30%                                |
| Public Services                  | 23                  |                                              | 2.37%                                |
| Energy – Critical Infrastructure | 24                  |                                              | 2.13%                                |
| Securities – Investment          | 29                  | Customer information, eKYC information, core | 1.82%                                |
| Education – EdTech               | 66                  | business data, data                          | 0.94%                                |
| Retail – E-commerce              | 107                 | extracted from the                           | 0.83%                                |
| Technology – Telecommunications  | 50                  | internal system, etc.                        | 0.26%                                |
| Healthcare – Pharmaceuticals     | 12                  |                                              | 0.08%                                |
| Manufacturing – Industry         | 18                  |                                              | 0.03%                                |
| Other                            | 84                  |                                              | 4.62%                                |

*Notes.* The source is Viettel Cyber Security (2026). “Proportion of Total Exposed Data” refers to each sector’s estimated share of the total exposed data documented by Viettel Cyber Security in 2025. In aggregate, Viettel Cyber Security reports approximately 4 billion records and 1.27 TB of exposed data.

Table 2, Table 3, Table 4, and Table 5 reveal three important patterns, as follows:

First, the number of documented incidents shows a clear upward trajectory over time. Although these figures do not necessarily capture all cases of personal data leakage, they still suggest that personal data breaches in Vietnam are not isolated events, but a recurring and expanding problem. The especially sharp increase in 2025 is striking and may indicate either a worsening situation, improved detection and reporting, or a combination of both.

Second, the breaches are distributed across a wide range of sectors, which suggests that the problem is systemic rather than confined to a few particularly vulnerable industries. The documented incidents indicate that the illegal trading of personal data is supported by leakages from both private and public-facing sectors and is not limited to any single segment of the economy.

Third, the seriousness of the problem lies not only in the number of incidents, but also in the scale and sensitivity of the data exposed. The reported breaches involved customer data, student information, transaction information, internal system data, sensitive documents, source code, and eKYC (Electronic Know Your Customer) information. In several cases, the volume of exposed data is extremely large, reaching millions or even tens of millions of records. This pattern is especially concerning because large and detailed datasets can enable identity theft, financial fraud, impersonation, and highly targeted scams on a broad scale.

At the same time, some caution is warranted in interpreting the notable personal data breaches in Vietnam from 2022 to 2025. The sectoral categories vary across the four years, and the reporting format is not fully uniform from year to year. Accordingly, the breaches are more useful for identifying broad trends, rather than for making exact year-to-year comparisons. Even so, they consistently show that personal data breaches in Vietnam are frequent, cross-sectoral, and often large-scale.

These incidents may just be the tip of the iceberg, as it seems almost impossible to document every case of personal data leakage. However, they sound the alarm about the severity of the illegal trading of personal data in Vietnam (Du, 2022; VNA, 2023; VNS, 2024). The illegal trading of personal data occurs so openly that a simple search using a few keywords immediately brings up numerous listings offering personal data for sale. Personal data is openly traded on social media platforms like Facebook and Telegram, where groups with thousands of members engage in such transactions. Additionally, those involved in the illegal trading of personal data also employ automated chatbots to sell personal data (Ka Mi, 2022b; Chi, 2023).

### **Some Notable Legal Cases Involving Personal Data Protection**

In contrast to the prevalence of illegal trading of personal data, legal proceedings involving personal data are relatively rare, particularly in civil cases. The authors present two civil cases to illustrate this anomaly. The first involved personal and family privacy, and the second was about the protection of customer information in the banking sector.

The first case is *A and P v. N* (“Judgment No. 03/2022/DS-PT,” 2022). This dispute primarily revolves around the rights to private life, personal secrecy, and family secrecy as stated in Article 38 of the 2015 Civil Code. In 2020, Ms. N filed a complaint with the Hau Giang Provincial Police, claiming that Mr. A and Mrs. P were continuously harassing her family. Ms. N documented 21 incidents to support her claims. The complaint also included private details about Mr. A and Mrs. P’s past lives without their consent. However, the local police found no sufficient basis to conclude that Mr. A and Mrs. P were causing the alleged disturbances.

In Judgment No. 03/2022/DS-PT dated 19 January 2022, the People's Court of Hau Giang Province ruled that Ms. N had infringed upon the personal and family privacy of the individuals involved, thus violating Article 38 of the 2015 Civil Code. Despite Ms. N's actions, the court found no evidence that she had spread the information to damage the reputation and dignity of Mr. A and Mrs. P, as she did not publicize the accusations broadly or in local media. Consequently, there was no basis for requiring Ms. N to publicly apologize at her place of residence. The court also ordered Ms. N to compensate Mr. A and Mrs. P for emotional distress with an amount equivalent to half the minimum wage (745,000 VND) per person.

The second case is *B v. Commercial Bank Q* ("Judgment No. 02/2020/DS-PT," 2020). This dispute focuses on the obligations of financial institutions to protect their customer information. In May 2018, Mrs. B deposited 19 billion VND at Commercial Bank Q. By August 2018, Mrs. B suspected the bank of disclosing her transaction details to Mrs. H, her sister-in-law. Despite assurances from the bank that no breach had occurred, Mrs. B continued to suspect that Mrs. G, a bank employee, as well as Mrs. H's high school friend, had leaked the information. In December 2018, Mrs. B requested an early withdrawal, resulting in a loss of nearly 895 million VND due to the difference between the regular and premature withdrawal interest rates. The bank had explained the confidentiality of deposits and the financial implications of early withdrawal; however, Mrs. B proceeded with her decision.

In Judgment No. 02/2020/DS-PT dated 19 February 2020, the People's Court of Hai Phong City found no evidence that the bank had disclosed any transaction details related to Mrs. B's 19 billion VND deposit. Consequently, the bank had not violated its duty to protect the confidentiality of customer information. The court dismissed Mrs. B's claim.

Efforts to prevent and combat crime and violations regarding the protection of personal data continue to face many challenges. Specifically, from the beginning of 2021 to February 2023, authorities prosecuted five cases involving thousands of gigabytes of personal data and billions of records being traded (Anh, 2023). In 2023, the Ministry of Public Security detected and investigated 16 incidents of data breaches in cyberspace (Quy, 2024). However, due to the lack of specific provisions defining the constituent elements of personal data trading activities, it is challenging to prove criminal offenses. The authors present four criminal cases related to the illegal trading of personal data.

The first case is *Prosecutor v. Q and P* (SGT, 2021). Q was a programmer at the Information and Communication Technology Company of Vietnam Electricity (EVNICT), which is part of the Vietnam Electricity Group (EVN). Q had access to a database containing the personal information of customers from local electricity companies. EVN regulations strictly prohibit any individual or organization from unauthorized access, theft, copying, extraction, exchange, or sale of customer data without EVN's consent.

In July 2017, Q and his wife P established an energy solutions company, with P serving as the director. The company specialized in developing software customized for clients in the information technology sector.

By the end of 2018, aware of some people's demand for EVN customer data, Q secretly copied personal information registered in EVN's database and stored it on his personal external hard drive. To facilitate the sale of this customer data, Q created websites that posted content related to customer groups. Prospective buyers could negotiate and purchase data packages, including names, phone numbers, and addresses of customers, with prices ranging from 200 to 1,000 VND per piece of information. From December 2018 to November 2020, Q and P sold data to over 100 buyers, illegally earning more than 279.2 million VND.

On 23 August 2022, the People's Court of Ha Noi City tried Q and P for the offense of "illegal transmission or use of information on computer networks or telecommunications networks" under Article 288 of the 2015 Criminal Code (as amended). However, due to new developments in the case, the court decided to return the case file for further investigation. In January 2023, the People's Court of Ha Noi City sentenced Q and P each to 30 months in prison, suspended, for the same offense under Article 288 of the 2015 Criminal Code (as amended).

The second case is *Prosecutor v. Q and others* (Thu, 2023). In 2019, seeking information for detective activities, T looked for sources to purchase phone location data, call histories, IP addresses, and bank account details. T knew A, the Deputy Director of the VNPT Information Security Center (part of the Vietnam Posts and Telecommunications Group – VNPT), could access phone-related data from VinaPhone, including subscriber details, call and message logs, and phone location. Consequently, T proposed buying this information, as well as similar data from other major network providers.

A used his privileges to access VinaPhone's system to extract data and collaborated with Q, a criminal police officer at the Long Bien District Police, to acquire and resell mobile phone user data to T. Specifically, Q facilitated the acquisition of personal data from Viettel and MobiFone subscribers by forging 142 official letters in the name of the Long Bien District Police. Q then sold the data of 1,007 phone users to A for 254 million VND.

On 15 March 2023, the People's Court of Ha Noi City sentenced Q to six years in prison for the offense of "illegal transmission or use of information on computer networks or telecommunications networks" under Article 288 of the 2015 Criminal Code (as amended), and for the offense of "fabricating an organization's seal or documents and use thereof" under Article 341 of the 2015 Criminal Code (as amended). Additionally, the court sentenced A to 30 months and T to 15 months in prison for the same offense of "illegal transmission or use of information on computer networks or telecommunications networks" under Article 288 of the 2015 Criminal Code (as amended).

The third case is *Prosecutor v. N and T* ("Judgment No. 628/2023/HS-PT," 2023). In April 2022, N started trading personal information, such as citizen identification numbers to fund his spending. He used Facebook to announce his need for such personal data. N discovered T's accounts on Zalo and Telegram selling personal information. They agreed on a price range from 2,000 to 3,000 VND per set of information, handling transactions via bank transfers. Over two months, N purchased 14,500 sets of personal information for 37 million VND from T. He then created three Facebook accounts to advertise and sell this data on various online platforms, tailoring prices based on the buyer's intended use of the information, ranging from 2,000 to 20,000 VND per set. N sold the personal information to 14 individuals for more than 244 million VND, netting an illicit profit of 207 million VND.

Furthermore, in June 2022, T and G purchased a download link containing personal data from a financial company for 5 million VND, which they then exploited and traded individually. Over two months, T sold 15,445 pieces of personal information to five individuals for 67 million VND, netting an illicit profit of 64.5 million VND. Similarly, G made an illicit profit of 500,000 to 600,000 VND and made about 20 million VND from selling the download link of the financial company.

On 28 August 2023, the People's Court of Thua Thien Hue Province sentenced T to six months and N to one year in prison for the same offense of "illegal transmission or use of information on computer networks or telecommunications networks" under Article 288 of the 2015 Criminal Code (as amended). G, whose actions did not constitute a criminal offense, was handed over for administrative penalties.

T appealed for a suspended sentence. In Judgment No. 628/2023/HS-PT dated 28 December 2023, the Superior People's Court in Da Nang held that the first-instance court's decision to sentence T to six months in prison reflected the humanitarian policy of the law. The appellate court denied T's request for a suspended sentence, stating that such a decision was necessary to effectively combat the rising trend of crimes in the fields of information technology and telecommunications. Consequently, the court rejected his appeal.

The fourth case is *Prosecutor v. D and others* ("Judgment No. 101/2025/HS-ST," 2025). From 2019 to December 2024, D collected and purchased more than 53 million items of personal data relating to individuals across Vietnam, including names, dates of birth, citizen identification numbers, telephone numbers, addresses, real estate information, social insurance information, bank account information, and other customer information. The total volume of data was approximately 306 GB. D purchased the data from multiple sources, including several co-defendants and other persons whose identities he could not fully recall. D then resold the same item of information to multiple buyers to maximize illicit profit. His principal customers were real estate brokers and persons advertising products and financial services. In total, D received more than VND 892 million and, after deducting purchase costs, obtained an illicit profit of more than VND 842 million. Several other co-defendants also participated in the illegal trading of millions of items of personal data.

In Judgment No. 101/2025/HS-ST dated 13 August 2025, the People's Court of Hue City sentenced D to 15 months in prison for the offense of "illegal transmission or use of information on computer networks or telecommunications networks" under Article 288 of the 2015 Criminal Code (as amended). The remaining co-defendants were convicted of the same offense and were sentenced to monetary fines ranging from VND 20 million to VND 25 million.

Administrative liability also plays an important role in the enforcement landscape of personal data protection, especially in consumer-facing digital services. The authors present two recent administrative cases concerning violations related to consumer data and consumer rights.

The first case concerns VNG Corporation (VNS, 2026). On 22 January 2026, following an inspection of compliance with consumer protection law, the Vietnam Competition Commission (VCC) imposed an administrative fine of VND 810 million on the company. Remarkably, the company failed to establish methods for consumers to choose the scope of information they agreed to provide and to express consent or refusal in relation to certain information. It also failed to provide consumers with a mechanism to choose whether their information could be used for advertising, marketing, and other commercial activities. In addition, the company was found to have included prohibited clauses in its general transaction conditions; as it failed to specify the applicable time of those conditions, failed to publicly disclose procedures for receiving and resolving consumers' complaints and requests, and failed to publicly disclose policies and mechanisms applicable to vulnerable consumers. The VCC required the company to cease the violations, review its policies, and ensure full compliance with consumer protection law. According to the VCC, the company subsequently cooperated with the authority and took steps to remedy a number of the identified shortcomings.

The second case concerns TikTok (VNS, 2026). On 22 January 2026, the VCC announced an administrative fine of VND 880 million against the company for several violations detected during an inspection of compliance with consumer protection law. Notably, the company did not provide a mechanism for consumers to choose whether their information could be used for advertising and marketing. The company was also found to have included prohibited clauses in its general transaction

conditions, provided incomplete information that could mislead consumers regarding the nature and characteristics of transactions, and failed to adopt appropriate procedures, methods, or measures for vulnerable consumers to exercise their rights to complain, request dispute resolution, and enjoy other consumer rights. The VCC required the company to cease the violations, review its policies, and ensure full compliance with consumer protection law.

## **REASONS FOR PERSONAL DATA BREACHES IN VIETNAM**

Personal data breaches in Vietnam are driven by three interrelated legal, socio-psychological, and technological factors. This tripartite configuration is supported by several complementary strands of scholarship and policy discourse. First, cyber-routine activity theory (CRAT), developed from routine activity theory, explains cybercrime through the interaction among motivated offenders, suitable targets, and the absence of capable guardianship. In the context of personal data breaches, motivated offenders are actors seeking to exploit data for unlawful gain; suitable targets include individuals and organizations that possess valuable and vulnerable personal data; and capable guardianship encompasses legal safeguards, individual awareness, and technical protection measures that can prevent or mitigate cyber offending (Vakhitova, 2025). Second, a quantitative study on the global geography of cybercrime identifies five interrelated sets of drivers – social, economic, political, technological, and cybersecurity factors. Its findings suggest that higher socio-economic development and stronger information and communication technology infrastructure are associated with greater cybercrime activity, while stronger governance conditions and better cybersecurity preparedness are associated with lower cybercrime risks (Chen et al., 2023). Third, public statements by representatives of Vietnam's Ministry of Public Security similarly distinguish between subjective and objective causes of illegal trading of personal data, including limited public awareness, weak compliance with personal data protection rules, the growing economic value of personal data, and inadequate cybersecurity safeguards (Nhung, 2025). Taken together, these theoretical and policy reflections support the analytical grouping adopted in this article. Legal reasons concern weaknesses in the regulatory and enforcement framework, including fragmented rules and limited compliance. Socio-psychological reasons concern human behavior and social conditions, such as low awareness of personal data protection, convenience-driven disclosure, and the attractiveness of personal data as a valuable target. Technological reasons concern both the opportunities created by digital transformation and the insufficiency of cybersecurity measures needed to prevent, detect, and respond to personal data breaches.

### **Legal Reasons**

Although the legal framework related to personal data protection has been revised in line with global trends, provisions on personal data protection remain scattered across various legal documents, ranging from the Constitution to laws, decrees, and circulars, giving rise to several specific issues as follows:

First, some legal documents stipulate the responsibilities of organizations and businesses in collecting and processing personal data, but these provisions are not comprehensive. For example, the 2018 Law on Cybersecurity outlines the responsibilities of service providers in cyberspace (Article 41). However, these provisions target specific organizations in cyberspace and lack a general framework for all entities involved in collecting and processing personal data. The 2023 Decree on Personal Data Protection outlines some obligations for data controllers and data processors, but it does not comprehensively cover the obligations of organizations and businesses handling personal data.

Second, the “notice and consent” mechanism – a fundamental model for collecting and processing personal data in cyberspace – has not proven effective. The 2015 Law on Network Information Security includes provisions for this mechanism (Article 17), but they are rudimentary. They mainly address the obligations of organizations and individuals collecting and processing data without considering the form, content, or methods for obtaining user consent, nor do they define what constitutes legally valid consent (Nguyen & Nguyen, 2022). Although the 2023 Decree on Personal Data Protection provides more detailed regulations regarding the consent of data subjects (Article 11), it still holds lower legal authority compared to the existing laws on the matter. In practice, the “notice and consent” mechanism fails to protect the personal data of users because it does not offer a truly meaningful choice. Often, the content of the notice is beyond the comprehension of the data subjects, rendering them unable to assess the privacy risks associated with disclosing their personal data to data processors.

Third, victims face significant difficulties in claiming damages for personal data breaches. In practice, under the burden of proof in civil litigation (Article 91 of the 2015 Civil Procedure Code), where the claimant bears the responsibility to provide evidence, victims cannot precisely identify the liable parties for data breaches, nor can they prove the actions that led to the data leakage. Additionally, proving the actual extent of the damage is also challenging.

Fourth, administrative penalties for violations related to personal data are scattered across various sector-specific legal documents (Chu, 2022). This fragmentation hinders the handling of violations when certain personal data-related infractions do not fall under the regulated sectors, thus lacking a comprehensive legal basis for enforcement. Moreover, the amount of the fines are too small to act as a deterrent and are not aligned with socio-economic development, leading malicious actors to willingly accept the penalties to engage in the illegal trading of personal data (Mi, 2022a; Dat, 2021).

Fifth, there is no specific offense related to personal data in the 2015 Criminal Code (as amended). Violations of personal information protection regulations can be prosecuted under two offenses specified in Articles 159 and 288, with a maximum imprisonment term of seven years. In practice, most cases involving the illegal trading of personal data are being investigated and prosecuted under these two articles. However, due to the lack of specific regulations defining the constituent elements of personal data trading activities, proving the crime remains challenging (Chu, 2022).

The 2025 Law on Personal Data Protection may address some of the above-mentioned reasons. In particular, it introduces more detailed provisions on the obligations of data controllers and data processors, as well as on the consent of data subjects. Administrative penalties for violations related to personal data have also been significantly increased. Nevertheless, because the 2025 Law on Personal Data Protection has only recently entered into force, its practical effectiveness in combating the illegal trading of personal data in Vietnam cannot yet be fully assessed.

### **Socio-psychological Reasons**

Awareness of cybersecurity risks among a significant portion of the population, as well as many organizations and businesses, remains limited. Specific common manifestations include the following instances:

First, a segment of the population is indifferent to privacy rights and shows little concern for protecting their personal data (Dang, 2023; Sen, 2020). For instance, consumers often receive messages, calls, and emails advertising free English courses, insurance packages, and beauty services. When they respond,

they are asked to provide some personal information. Some consumers readily provide their information without proper consideration of how it will be used, leading to data leaks beyond their awareness (NK, 2022). Additionally, most personal information, such as birth dates, schools, workplaces, and residences, is often publicly listed on social media accounts by the users themselves. The more diligently someone updates their social media activities, the higher the risk of personal information exposure (VNS, 2023).

Second, some users lack caution when interacting online (Huyen & Huong, 2024). For example, malicious actors create or exploit websites with appealing content to attract users. When users access these sites, malware is silently installed on their computers and smart devices, collecting information without their knowledge. Malware distribution is also carried out via email. Malicious actors impersonate email addresses of officials or colleagues within an organization to send files with requests for opinions or work exchanges. In such cases, the malicious actors often thoroughly research the names and positions of people within the organization before distributing malware via email.

Additionally, malicious actors create fake login pages (Huyen & Huong, 2024). These pages closely resemble the login interfaces of legitimate service providers. If the victim is not vigilant and enters the login credential, it is sent to malicious actors instead of the legitimate service providers.

Another method is through free software (Huyen & Huong, 2024). Some free software available on the internet, especially those from ambiguous or unverified sources, may contain embedded malware. When users download and install this software, they inadvertently install malware on their devices, which then silently collects their personal data.

Third, some users know about their privacy rights, but are still willing to trade their privacy for economic benefits (often minimal) or mere convenience (Kiet, 2024; Du, 2022). This phenomenon is often described as the privacy paradox, in which individuals believe that they should be concerned about privacy, yet still disclose their personal data so long as doing so offers some perceived advantage (Brown, 2001). Consequently, in commercial settings, a significant part of the erosion of individual privacy takes place with the individual's own consent (Barnes, 2006). For example, malicious actors create fake pages impersonating brands and post content about valuable giveaways to attract thousands of people to comment with any information the fake page requests (Quy, 2023). The privacy paradox also leads to a more serious consequence, namely the failure of privacy self-management. Privacy self-management is a regulatory model in which individuals make various decisions and choices concerning their own privacy through the notice-and-consent mechanism, thereby enabling them to weigh the costs and benefits of sharing their personal data. However, the privacy paradox suggests that granting more control to data subjects does not always result in more effective privacy protection. This creates a vicious cycle in which individuals continue to be entrusted with managing their own privacy while still remaining concerned about the security of their personal data (Solove, 2013, 2021).

Fourth, many organizations and businesses do not recognize their responsibility to protect personal data or the potential consequences of data breaches, or providing data to third parties (VNS, 2024). Many businesses easily allow their partners to access customer information, while confidentiality agreements within the supply chain are often lax, affecting both the business and customers when data leaks occur (VNA, 2023). Some data management employees in organizations and businesses even collude with third parties to trade personal customer data.

## **Technological Reasons**

Organizations and businesses in Vietnam have not implemented measures to secure data which commensurate with the scale of their personal data resources. Specific common issues include the following:

First, many organizations and businesses collecting personal data lack adequate data protection measures. They do not have appropriate management and technical measures to safeguard the personal data they collect, especially those classified as medium or small-scale outfits. Their ability to respond to threats remains weak (Huyen & Huong, 2024). These organizations and businesses lack the necessary resources to ensure cybersecurity and have not fully controlled the risks of cybersecurity breaches. Their information systems are capable of collecting, processing, and storing personal data, but fail to ensure security, making them vulnerable to attacks and exploitation by malicious actors (VNISA, 2022).

Second, some businesses have security systems, but fail to update them based on real-world incidents of data breaches, creating conditions for personal data leaks. For example, some businesses might invest in a four-layer information security infrastructure, which include on-site forces, professional monitoring and protection organizations or businesses, independent periodic evaluation organizations or businesses, and connectivity and information sharing with the national monitoring system. However, if they do not update their knowledge of new cyberattack techniques, these businesses will struggle to prevent and defend against hacker intrusions (NK, 2022).

Third, when data breaches occur, organizations and businesses often do not notify the specialized cyber information incident response units to mitigate the effects and do not take timely corrective actions, or inform the affected individuals and organizations (Huyen & Huong, 2024; VNS, 2024).

Fourth, cybersecurity personnel in medium and small businesses are often part-time, leading to a lack of both quantity and quality. Their cybersecurity knowledge and skills are not regularly updated, while cyberattack methods become increasingly complex (Huyen & Huong, 2024; Van, 2022).

Fifth, there is a lack of companies providing technical solutions. Currently, there are 85 businesses operating in the field of cybersecurity, including four state-owned corporations, 54 joint-stock companies, and 27 limited liability companies. Among these, 72 companies are licensed to import products, 13 are licensed to manufacture products, and 56 are licensed to provide services. This number is still small compared to the demand, not to mention the capability of these businesses to meet the requirements (Huyen & Huong, 2024).

## **LEGAL AND POLICY SOLUTIONS TO FIGHT AGAINST ILLEGAL TRADING OF PERSONAL DATA IN VIETNAM**

The enactment of the 2025 Law on Personal Data Protection has strengthened the legal framework on personal data. However, because this law only took effect on 1 January 2026, its effectiveness in preventing and combating the illegal trading of personal data remains to be thoroughly assessed. Nevertheless, despite the promulgation of the 2025 Law on Personal Data Protection, several legal and policy measures remain necessary to further strengthen the prevention of, and fight against the illegal trading of personal data. This will be discussed as follow:

First, legal terminology related to personal data and its protection should be standardized across existing specialized laws and the 2025 Law on Personal Data Protection. This measure will help unify the legal understanding about regulations regarding personal data, enabling organizations and individuals to clearly define the scope of their obligations in protecting personal data. As a result, it will also lead to the consistent application of the law and the effective safeguarding of personal data in practice, thereby enhancing the effectiveness and efficiency of state management in this matter.

Second, criminal sanctions for violations related to personal data should be strengthened. While administrative penalties have become more severe, criminal sanctions have remained unchanged. This creates a disparity between the deterrent effect of administrative and criminal measures. In practice, the increasing number of personal data breaches indicates that current criminal sanctions are insufficient to deter and prevent the illegal trading of personal data.

It is necessary to enhance educational initiatives focused on personal data protection to raise awareness of cybersecurity risks and prevent unwanted personal data exposure (VNA, 2024). The authors commend the efforts of the University of Social Sciences and Humanities (Vietnam National University, Hanoi) for issuing the Digital Competency Framework (DCF) for students (Thuy Dzung, 2024). This DCF includes seven competency groups with 26 criteria, as follows: (1) devices and software operations, (2) information and data exploitation, (3) communication and collaboration in the digital environment, (4) safety and digital well-being, (5) digital content creation, (6) learning and development of digital skills, and (7) application of digital competency in professional fields (Tran & Do, 2021).

On 24 January 2025, the Ministry of Education and Training promulgated Circular No. 02/2025/TT-BGDDT on the DCF for Learners. This DCF consists of six competency domains with 24 component competencies and is divided into four levels, from basic to specialized, across eight levels. In particular, “protecting personal data and privacy” is a component competency within the Safety domain. This competency component equips learners with the knowledge and skills to protect personal data and safeguard privacy in digital environments; to understand how to use and share personally identifiable information safely, and to be able to protect themselves and others; and to understand how digital services use Privacy Policies to inform users about methods of personal data use. It is divided into eight levels with different objectives, ranging from identifying simple ways to protect personal data and privacy in digital environments (Level 1), to creating solutions to solve complex problems involving many interacting factors related to protecting personal data and privacy in digital environments (Level 8). This Circular will help educational institutions throughout the country to develop and assess the digital competence of learners, as well as to ensure consistency in digital competence requirements for learners. Specifically, it will contribute to a more effective “notice and consent” mechanism by fostering a generation of young Internet users capable of understanding privacy policies and notices.

Integrating digital competency into the curriculum at various educational levels is essential for training responsible citizens in the digital age. These individuals will be equipped with the digital skills needed to confidently engage in the online environment in a safe, healthy, and effective manner (VNA, 2021, 2022).

## CONCLUSION

The illegal trading of personal data poses a significant challenge to Vietnam's efforts to safeguard individual privacy and ensure the integrity of its thriving digital economy. Before the promulgation of the 2025 Law on Personal Data Protection, Vietnam had made considerable progress in establishing a legal framework for personal data protection. However, inconsistencies within this framework and inadequacies in enforcement complicated the fight against the illegal trading of personal data. Persistent vulnerabilities across legal, socio-psychological, and technological domains underscored the need for a more comprehensive and effectively implemented regulatory approach.

The enactment of the 2025 Law on Personal Data Protection marks an important step toward addressing the aforementioned issues. This law has the potential to consolidate scattered regulations and align Vietnam's legal framework with international standards. Nevertheless, as existing specialized laws remain in effect, their practical effectiveness will depend on how coherently they are implemented and enforced in practice. It is essential to standardize legal terminology to fully resolve the lack of consistency within Vietnam's legal framework for personal data protection. Additionally, stricter criminal sanctions are indispensable to address violations related to personal data. Strengthening educational initiatives, particularly in digital competency, is also crucial to raise public awareness of personal data protection and empower citizens to navigate the digital environment responsibly. Although the fight against the illegal trading of personal data is undoubtedly an uphill battle, the 2025 Law on Personal Data Protection may represent an important part of the solution. Whether Vietnam has truly found the key to the puzzle, however, will ultimately depend not only on the laws as drafted and enacted, but also on its effectiveness in enforcement.

## ACKNOWLEDGMENT

This research is funded by the University of Economics and Law, Vietnam National University Ho Chi Minh City, Ho Chi Minh City, Vietnam.

The authors declare that they have no conflict of interest.

## CONFLICT OF INTEREST STATEMENT

The author reported no conflicts of interest for this work and declare no potential conflict of interest concerning the research, authorship, or publication of this article

## REFERENCES

- Anh, V. (2023, June 7). *10 big data leakage cases detected in Q1/2023*. Vietnamnet Global. <https://vietnamnet.vn/en/10-big-data-leakage-cases-detected-in-q1-2023-2152054.html>
- Anh, V. (2024, August 2). *Personal data breaches in Vietnam continue to be common*. VietnamNet Global. <https://vietnamnet.vn/en/personal-data-breaches-in-vietnam-continue-to-be-common-2304618.html>
- Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9). <https://doi.org/10.5210/fm.v11i9.1394>

- Brown, B. (2001). *Studying the internet experience*. HP Laboratories Bristol.
- Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., & Gao C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*, 10(7). <https://doi.org/10.1057/s41599-023-01560-x>
- Chi, Y. (2023). *Mua bán dữ liệu cá nhân online: Ngày một tinh vi* [The online trading of personal data: Becoming increasingly insidious]. Public Security News.
- Chu, H. (2022). Legal framework for personal data protection in Vietnam. In T. Phan & D. Damian (Eds.), *Smart cities in Asia: Regulations, problems, and development* (pp. 91–101). Springer. [https://doi.org/10.1007/978-981-19-1701-1\\_8](https://doi.org/10.1007/978-981-19-1701-1_8)
- Dat, T. (2021, Disember 16). *Heavy sanctions needed to prevent illegal trade of personal data*. VietNamNet.
- Dang, H. (2023). *Vietnamese indifferent to information security*. VietNamNet Global.
- Du, P. (2022). *Personal data theft rampant, says public security ministry*. VnExpress International.
- Dzung, T. (2024). *VNU-USSH: The first university to establish a Digital Competency Framework for students*. VNU University of Social Sciences and Humanities. <https://ussh.vnu.edu.vn/en/news/activities/vnu-uss-h-the-first-university-to-establish-a-digital-competency-framework-for-students-20689.html>
- Huyen, P., & Huong, N. (2024, Julai 29). *Hang loạt thu đoan thu thap trai phep du lieu ca nhan (bai 2) [Tactics for illegally collecting personal data (part 2)]*. Public Security News. <https://cand.com.vn/Hoat-dong-LL-CAND/hang-loat-thu-doan-thu-thap-trai-phep-du-lieu-ca-nhan-bai-2--i724847/>
- Huong, N. (2020). *Du lieu ca nhan dang bi mua ban, thu thap [Personal data is being traded and collected]*. Public Security News. <https://cand.com.vn/Xa-hoi/Du-lieu-ca-nhan-dang-bi-mua-ban-thu-thap-i553619/>
- Judgment No. 02/2020/DS-PT, (People’s Court of Hai Phong City 2020). [https://congbobanan.toaan.gov.vn/5ta464838t1cvn/An\\_so\\_\\_02\\_OANH\\_\\_NGAN\\_HANG\\_QUOC\\_DAN\\_MA\\_HOA.pdf](https://congbobanan.toaan.gov.vn/5ta464838t1cvn/An_so__02_OANH__NGAN_HANG_QUOC_DAN_MA_HOA.pdf)
- Judgment No. 03/2022/DS-PT, (People’s Court of Hau Giang Province 2022). [https://congbobanan.toaan.gov.vn/5ta869865t1cvn/BA\\_DSPT\\_032022\\_PHA\\_TUAN\\_ANHNGOAN.pdf](https://congbobanan.toaan.gov.vn/5ta869865t1cvn/BA_DSPT_032022_PHA_TUAN_ANHNGOAN.pdf)
- Judgment No. 101/2025/HS-ST, (People’s Court of Hue City 2025). [https://congbobanan.toaan.gov.vn/5ta1960426t1cvn/sample\\_4.pdf](https://congbobanan.toaan.gov.vn/5ta1960426t1cvn/sample_4.pdf)
- Judgment No. 628/2023/HS-PT, (Superior People’s Court in Da Nang 2023). [https://congbobanan.toaan.gov.vn/5ta1392036t1cvn/Ban\\_an\\_so\\_6282023HSPT\\_ngay\\_28122023\\_Tran\\_Nhat\\_T\\_\\_CT\\_PHAM\\_VIET\\_CUONG.pdf](https://congbobanan.toaan.gov.vn/5ta1392036t1cvn/Ban_an_so_6282023HSPT_ngay_28122023_Tran_Nhat_T__CT_PHAM_VIET_CUONG.pdf)
- Keck, M. (2021). *The role of data protection in the digital economy*. UNCDF. <https://policy.accelerator.uncdf.org/s/EN-UNCDF-Brief-Data-Protection-2021.pdf>
- Kemp, S. (2024). *Digital 2024: Vietnam*. DataReportal.
- Kiet, A. (2024). *Vietnam strengthens protection of personal data in cyberspace*. Hanoitimes. <https://hanoitimes.vn/vietnam-strengthens-protection-of-personal-data-in-cyberspace-327121.htm>
- Mi, K. (2022, February 23a). *Legal gaps exist on protection of personal data in Vietnam*. VietnamNet Global.
- Mi, K. (2022 February 21b). *VN to crack down on trading of personal data online*. VietnamNet Global <https://vietnamnet.vn/en/vn-to-crack-down-on-trading-of-personal-data-online-816735.html>
- Nguyen, T. L., & Nguyen, N. H. (2022). “Thông báo và đồng ý” trong thu thập, xử lý dữ liệu cá nhân [“Notice and Consent” in the collection and processing of personal data]. *Tap chi Kiem sat Journal of Procuracy*, 61(23), 58–63.
- Nam, D. (2016, August 1). *Vietnam Airlines under cyber-attack since 2014: Security group*. VnExpress.

- NK. (2022). *Cac doanh nghiệp cần làm gì khi bị lộ lọt dữ liệu, thông tin cá nhân của người dùng?* [What should businesses do when users' personal data and information are leaked?]. *Electronic Journal of Information and Communications Technology*.
- Nhung, T. (2025). *Leaked data fuels smarter scams: Vietnam drafts personal data law*. VietNamNet. <https://vietnamnet.vn/en/scammers-use-leaked-data-to-fool-unsuspecting-victims-2395190.html>
- Quynh, V. (2020). *Dữ liệu cá nhân hay thông tin cá nhân?* [Personal data or personal information?]. People's Deputies. <https://daibieunhandan.vn/du-lieu-ca-nhan-hay-thong-tin-ca-nhan-post256280.html>
- Quy, L. (2023). *'Hố đen' dữ liệu cá nhân* [The 'black hole' of personal data]. VnExpress.
- Quy, L. (2024). *Online sale of personal data organized and widespread in Vietnam*. VnExpress. <https://e.vnexpress.net/news/news/online-sale-of-personal-data-organized-and-widespread-in-vietnam-4771159.html>
- Rahman, F. (2025). Safeguarding personal data in the public sector: Unveiling the impact of the new personal data protection act in Indonesia. *UUM Journal of Legal Studies*, 16(1), 1–18. <https://doi.org/10.32890/uumljs2025.16.1.1>
- Sen. (2020). *Sharing personal data no big deal to Vietnamese: Survey*. VnExpress International.
- SGT. (2021, May 20). *Head of tech firm prosecuted for trading in large amount of personal data*. VietnamNet Global. <https://vietnamnet.vn/en/head-of-tech-firm-prosecuted-for-trading-in-large-amount-of-personal-data-738095.html>
- Sholehuddin, N., Miskam, S., Shahwahid, F. M., Aziz, T. N. R. A., & Mansor, N. (2024). A comparative legal analysis on personal data protection laws in selected ASEAN countries. *Journal of Muwafaqat*, 7(1), 23–38. <https://doi.org/10.53840/muwafaqat.v7i1.166>
- Solove, D. J. (2013). Privacy self-management and the consent dilemma. *Harvard Law Review*, 126(7), 1880–1903. [https://harvardlawreview.org/wp-content/uploads/2013/05/vol126\\_solove.pdf](https://harvardlawreview.org/wp-content/uploads/2013/05/vol126_solove.pdf)
- Solove, D. J. (2021). The myth of the privacy paradox. *George Washington Law Review*, 89(1), 1–51. <https://www.gwlr.org/wp-content/uploads/2021/01/89-Geo.-Wash.-L.-Rev.-1.pdf>
- Son, T. (2018). *Vietnam's tech giant VNG apologizes after alleged data breach affecting 163mn accounts*. Tuoi Tre News.
- Thu, H. (2023). *Police officer, telecom staff sell thousands' personal data*. VnExpress.
- The Economist. (2017). *Data is giving rise to a new economy*. The Economist. <https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy>
- The Saigon Times. (2023, June 8). *Over 1,300GB of personal data illegally collected and traded*. The Saigon Times.
- Tran, D. H., & Do, V. H. (2021). Digital literacy framework for Vietnam students in the digital transformation. *Tap chi Thong tin va Tu lieu* [Journal of Information and Documentation], 2021(1), 12–21. <https://vjol.info.vn/index.php/VJIAD/article/view/58291/48751>
- Toan, L. M. (2021). *Illegal trading of personal data difficult to control*. VietnamNet Global.
- Vakhitova, Z. I. (2025). Cyber-routine activity theory. In Hendry N Pontell (Ed.), *Oxford research encyclopedia of criminology and criminal justice*. Oxford University Press. <https://doi.org/10.1093/acrefore/9780190264079.013.784>
- Van, L. (2022, September 1). *Vietnam faces cybersecurity manpower shortage*. The Saigon Times. <https://english.thesaigontimes.vn/vietnam-faces-cybersecurity-manpower-shortage/>
- Viettel Cyber Security. (2023). *Báo cáo tình hình nguy cơ an toàn thông tin năm 2022* [Report on the situation regarding information security risks in 2022]. <https://blog.viettelcybersecurity.com/bao-cao-tinh-hinh-nguy-co-attt-nam-2022-viettel-threat-intelligence/>
- Viettel Cyber Security. (2024a). *Báo cáo tình hình nguy cơ an toàn thông tin tại Việt Nam 6 tháng đầu năm 2024* [Report on the situation regarding information security risks in Vietnam in the

- first half of 2024*]. <https://blog.viettelcybersecurity.com/bao-cao-tinh-hinh-nguy-co-mat-at-tai-viet-nam-6-thang-dau-nam-2024/>
- Viettel Cyber Security. (2024b). *Bao cao tinh hinh nguy co mat an toan thong tin tai Viet Nam nam 2023 [Report on the situation regarding information security risks in Vietnam in 2023]*. <https://blog.viettelcybersecurity.com/tinh-hinh-nguy-co-mat-at-tai-viet-nam-nam-2023/>
- Viettel Cyber Security. (2025). *Bao cao tinh hinh nguy co an toan thong tin tai Viet Nam nam 2024 [Report on the situation regarding information security risks in Vietnam in 2024]*. <https://blog.viettelcybersecurity.com/bao-cao-tinh-hinh-nguy-co-at-tai-viet-nam-nam-2024/>
- Viettel Cyber Security. (2026). *Bao cao tinh hinh nguy co an toan thong tin tai Viet Nam nam 2025 [Report on the situation regarding information security risks in Vietnam in 2025]*. <https://viettelsecurity.com/vi/resource-report/bao-cao-tinh-hinh-nguy-co-at-tai-viet-nam-nam-2025/>
- VNA. (2021, January 20). *Cybersecurity to be included in high school curriculum*. VietnamPlus.
- VNA. (2022, October 13). *Vietnam promotes digital literacy*. VietnamPlus.
- VNA. (2023, June 4). *Officer warns of data breach trend in Vietnam*. VietnamPlus.
- VNA. (2023, February 25). *PM urges basic, comprehensive reform in digital transformation*. Nhan Dan.
- VNA. (2024, June 28). *Public awareness a decisive factor in digital transformation: PM*. Nhan Dan.
- VNISA. (2022). *International Conference Vietnam Cyber Security Day 2022*. <https://vnisa.org.vn/en/international-conference-vietnam-cyber-security-day-2022/>
- VNS. (2023, November 7). *Legal framework essential to protect personal data, drive digital economy: Experts*. Vietnam News.
- VNS. (2023, August 23). *Personal information often stolen from social media*. Vietnam News.
- VNS. (2024, August 30). *Better cybersecurity needed to protect data*. VietnamNet Global.
- VNS. (2024b, August 1). *Rampant personal data threats prompt calls for enhanced cybersecurity measures*. VietnamNet Global.
- VNS. (2026, January 23). *Zalo and TikTok face huge fines for violations of consumer rights*. Vietnam News.