© IJARW | ISSN (O) - 2582-1008
August 2026 | Vol. 8 Issue. 2
www.ijarw.com

PROHIBITED ACTS IN DATA ACTIVITIES UNDER VIETNAMESE LAW: FOUNDATIONS FOR THEIR ESTABLISHMENT AND SELECTED ISSUES FOR IMPROVEMENT

Nguyễn Thị Thùy Giang

Department of Law, TNU - University of Sciences, Thai Nguyen 25000, Vietnam

ABSTRACT

This article clarifies the theoretical and legal foundations of the provisions on prohibited acts in data activities under Vietnamese law, focusing on Article 10 of the 2024 Law on Data and its relationship with Article 7 of the 2025 Law on Personal Data Protection. Using doctrinal analysis, systemic analysis, and cross-statute comparison, the article argues that the core function of these prohibitions is to establish legal limits on activities capable of infringing data sovereignty and security, the integrity and availability of data, privacy, and the lawful rights and interests of agencies, organizations, and individuals; post-violation sanctions serve as mechanisms for enforcing those limits. Four groups of acts under the Law on Data are examined: abusing data activities to infringe legally protected interests; obstructing, attacking, appropriating, or destroying databases and information systems; forging, intentionally falsifying, deleting, or damaging data in databases of the political system; and intentionally providing inaccurate data or failing to provide data as required by law. On that basis, the article clarifies the allocation of regulatory functions between general data law and personal data protection law, and proposes improvements concerning criteria for identifying prohibited conduct, fault requirements, coordination in the application of law, and measures to ensure traceability, auditability, and remediation of data incidents.

Keyword: data; prohibited acts; data governance; personal data protection; data security; Vietnamese law.

1. INTRODUCTION

In the digital economy, data have moved beyond being a by-product of administrative or transactional activities to become a critical input for public governance, production, business, scientific research, and service delivery. The capacity to collect, connect, analyze, and reuse data creates substantial socioeconomic value and, in turn, changes how the State makes decisions and how enterprises organize their operations. The 2024 Law on Data recognizes data as a resource and directs the development of data into an asset, thereby laying the groundwork for a data market and a national data ecosystem [5].

The very characteristics that create the value of data also increase legal risks. Data can be copied rapidly, combined from multiple sources, transferred across borders, and used for purposes different from those originally intended. A minor error in source data may be replicated across multiple systems; an incident that disrupts a database may simultaneously affect thousands of procedures, transactions, or decisions; and an appropriated dataset may continue to be exploited even after the original copy has been recovered. These features require data governance to go beyond technical obligations and post-harm compensation mechanisms by identifying in advance conduct that falls outside acceptable limits.

On 30 November 2024, the National Assembly adopted Law No. 60/2024/QH15 on Data, effective from 1 July 2025. Article 10 sets out four groups of prohibited acts, forming a general layer of protection for the development, protection, governance, processing, and use of data [5]. Subsequently, Law No. 91/2025/QH15 on Personal Data Protection, effective from 1 January 2026, separately provided for seven prohibited acts in the processing and protection of personal data [8]. The coexistence of these two sets of provisions indicates that Vietnamese law is moving from a fragmented, information-system-

based approach toward a more comprehensive framework for data regulation.

This article addresses three principal questions: first, what theoretical grounds justify the establishment of prohibited acts in data activities; second, how the current Vietnamese legal system establishes and allocates the regulation of such acts; and third, what elements should be improved to ensure consistent application, prevent risks, and avoid criminalizing or over-penalizing ordinary technical or professional errors. The article employs doctrinal analysis, systemic analysis, legal interpretation, and comparison among the Law on Data, the Law on Personal Data Protection, and the laws on cybersecurity, cyberinformation security, civil liability, and criminal liability.

2.FOUNDATIONS FOR ESTABLISHING PROHIBITED ACTS IN DATA ACTIVITIES

2.1. Theoretical foundations for establishing prohibited acts

In legal theory, a prohibitory rule is a form of mandatory legal norm that identifies conduct in which legal subjects may not engage because it is capable of harming social relations and interests protected by law [11]. Unlike empowering rules or rules imposing positive duties, a prohibition establishes a negative boundary: once conduct satisfies the legally prescribed elements, the subject must refrain from it, irrespective of any claimed economic benefit or technical utility. In data activities, prohibitory regulation is particularly significant because many forms of harm may emerge rapidly, spread widely, and prove difficult to remedy fully.

The first foundation for prohibitory regulation is the need to protect multiple categories of interests through a single mechanism. Data may be connected with national interests, national defense and security, public order and safety, the public interest, trade secrets, privacy, honor and dignity, property, and other lawful rights and interests. A single data-related act may infringe several protected interests at once. For example, appropriating identification data may violate an individual's privacy, facilitate property fraud, and undermine trust in an electronic identification system. This multiplicity of protected interests makes prohibitions in data law inherently interdisciplinary and requires their interpretation in connection with civil law, cybersecurity law, cyberinformation security law, the law on protection of state secrets, and criminal law.

The second foundation is the risk-amplifying nature of digital data. Digital data can be copied at minimal cost, aggregated into detailed profiles, transmitted at high speed, and reused repeatedly without the affected subject being aware. The intangible nature of data means that appropriation or falsification may leave no visible trace comparable to interference with tangible property. In the absence of processing logs, provenance information, and authentication mechanisms, proving who modified, copied, supplied, or deleted data becomes difficult. The scope of protection must therefore extend to data content, integrity, confidentiality, availability, traceability, and the reliability of the entire processing chain [3].

The third foundation is the asymmetry of capacity and information among actors in the data ecosystem. Database administrators, platform enterprises, data-processing service providers, and organizations holding large datasets often possess substantially greater technical control and knowledge than individuals, users, or organizations dependent on those data. Where one party can unilaterally alter, conceal, block access to, or repurpose data, contractual arrangements alone may not adequately protect the weaker party. Prohibitory rules therefore operate as a means of correcting disparities in data power by setting limits that agreements between the parties cannot lawfully override.

The fourth foundation is prevention. Many acts in data activities are dangerous from the moment they are carried out, even if final material harm has not yet occurred or cannot yet be fully quantified. Attacking a database, intentionally falsifying data used for decision-making, or selling personal data all create a serious risk of infringement. The law need not wait until actual harm occurs before intervening. The value of prohibition lies in establishing “red lines” that permit prevention, suspension, restoration orders, or the imposition of legal liability once unlawful conduct is identified.

Nevertheless, a prohibitory rule is justified only when it satisfies requirements of legal certainty, necessity, and proportionality. If concepts are framed too broadly, every data-entry error, delayed update, or technical interruption could be

treated as a prohibited act. Conversely, intervention only after serious harm has materialized would weaken the preventive function of the law. The theoretical basis of prohibitions in data activities therefore rests on balancing strong protection of essential interests with sufficiently clear limits on intervention so as not to impede lawful data activities, innovation, and responsible data sharing.

2.2. Constitutional and civil-law foundations

The highest legal foundation for prohibitions in data activities is found in the 2013 Constitution. The Constitution recognizes and protects human rights and citizens' rights, and provides that restrictions on such rights may be imposed only by law where necessary for reasons of national defense, national security, public order and safety, social morality, or public health [1]. At the same time, the inviolability of private life, personal and family secrets, and the right to confidentiality and security of correspondence, telephone communications, telegraphs, and other forms of private communication form the direct constitutional foundation of personal data protection law.

The 2015 Civil Code gives effect to this foundation through provisions on the right to private life, personal secrets and family secrets; image rights; the protection of honor, dignity, and reputation; compensation for damage; and other civil remedies [2]. Data may reflect, store, or reconstruct elements associated with a person's identity and property. From this perspective, the collection, disclosure, use, falsification, or loss of data goes beyond a technical issue and may directly infringe civil rights. Prohibitions under data law add a preventive and governance-oriented layer of protection, while civil law provides remedies such as cessation of the infringement, apology, public correction, restoration of the original position, and compensation for damage.

Beyond privacy, the civil-law foundation of prohibitions also concerns property rights and lawful economic interests. The Law on Data directs the development of data into an asset, but does not equate all data with property that may be freely traded [5]. The economic value of data depends on their origin, control rights, processing purposes, the rights of relevant subjects, and restrictions under sector-specific law. Protecting the data market must therefore be associated with prohibiting the unlawful appropriation, destruction, forgery, or exploitation of data. A sustainable market can operate only where data provenance is verifiable, the rights of the parties are defined, and fraudulent or appropriative conduct is excluded.

2.3. Sector-specific legal foundations and the relationship among relevant laws

The 2024 Law on Data is a framework statute governing the development, protection, governance, processing, and use of data; data products and services; and the rights, obligations, and responsibilities of relevant agencies, organizations, and individuals. Article 5 establishes principles of legal compliance, protection of human rights and citizens' rights, national interests, the public interest, and data security and safety, as well as efficiency in data connection, sharing, exploitation, and use. Article 6 recognizes data as a resource and provides for State policies to develop data into an asset. Against that background, Article 10 establishes four groups of prohibited acts [5].

Decree No. 165/2025/ND-CP details a number of provisions and measures for implementing the Law on Data, clarifying the criteria for important data and core data, data-processing activities, data protection, and cross-border data processing [6]. Decree No. 278/2025/ND-CP governs mandatory data connection and sharing among agencies within the political system, emphasizing a single trusted source of data, standardization, synchronization, authorization, supervision, and traceability in data sharing [7]. These decrees do not add prohibited acts beyond those prescribed by statute, but they provide technical and governance standards for assessing the seriousness and consequences of conduct affecting data.

For personal data, the 2025 Law on Personal Data Protection is the sector-specific statute. Article 7 establishes seven prohibited acts: processing personal data to infringe the State, national defense and security, public order and safety, or lawful rights and interests; obstructing personal data protection activities; abusing personal data protection activities to violate the law; unlawfully processing personal data; using another person's personal data, or allowing another person to use one's own personal data, to commit unlawful acts;

buying or selling personal data, except where otherwise provided by law; and appropriating, intentionally disclosing, or causing the loss of personal data [8]. Decree No. 356/2025/ND-CP further specifies data-subject rights, consent, data transfers, big-data processing, sector-specific data protection, and compliance mechanisms [9].

The Law on Data and the Law on Personal Data Protection stand in a general-to-special relationship determined by the type of data concerned. Where conduct involves personal data, the specific requirements governing the lawful basis for processing, data-subject rights, consent, impact assessment, and cross-border data transfers should take priority. If the same conduct also infringes a database, an information system, or important data, provisions of the Law on Data, cybersecurity law, and cyberinformation security law should also be invoked to assess all affected legal interests. Concurrent application of several statutes does not mean duplicative punishment; the competent authority must identify the conduct, consequences, protected interests, and corresponding legal basis for liability.

In addition, the 2015 Law on Cyberinformation Security protects the integrity, confidentiality, and availability of information, while the 2018 Law on Cybersecurity safeguards national security, public order and safety, and lawful rights and interests in cyberspace [3], [4]. The Criminal Code and administrative-sanctions legislation provide penalties for conduct that reaches the statutory threshold of an administrative violation or a criminal offense [10]. Article 10 of the Law on Data is thus primarily a rule defining the boundaries of permissible conduct; the imposition of a specific sanction still requires reference to the provisions on constituent elements, jurisdiction, procedure, and penalty levels in the relevant legal instruments.

3. LEGAL IDENTIFICATION OF PROHIBITED ACTS IN DATA ACTIVITIES

3.1. Abusing data activities to infringe legally protected interests

Clause 1, Article 10 of the Law on Data prohibits the abuse of data processing, data governance, and the development, trading, and circulation of data products and services to infringe national and ethnic interests, national defense and security, public order and safety, the public interest, and the lawful rights and interests of agencies, organizations, and individuals [5]. This is the broadest provision in Article 10 because it covers technical, governance, and commercial activities throughout the entire data lifecycle.

The central element of this provision is "abuse." In essence, a subject uses an activity that may otherwise be lawful—such as processing, analysis, brokerage, supply, or circulation of a data product—as a means of causing harm. This does not mean that every data activity producing an adverse effect automatically falls within Clause 1. It is necessary to establish a link between the exploitation of data characteristics, access rights, or a position of data control and the purpose or method of infringing a protected interest. This element will ordinarily be associated with intentional fault, although the provision does not expressly prescribe the form of fault.

The conduct may take various forms: using transaction data to manipulate a market; exploiting location data to conduct unlawful surveillance of an individual; supplying data-analytics services for fraudulent purposes; building a data repository from unlawful sources; or circulating a data product known to contain forged or inaccurate information capable of causing harm. The common feature is that data activities cease to serve lawful governance, innovation, or exchange and instead become an instrument of infringement.

The flexibility of the provision enables it to encompass emerging methods of violation, but also creates a need for specific guidance on the terms "abuse," "infringe," and the scope of the "public interest." Without application criteria, the boundary between prohibited conduct and legally permissible but risk-bearing data processing may become uncertain. At a minimum, application should consider four factors: the subject's legal status and access rights; the actual purpose of the activity; the type of data and the interests affected; and the degree to which the subject knew or could reasonably foresee the consequences.

3.2. Unlawfully obstructing or preventing data processing and governance; attacking, appropriating, or destroying databases and information systems

Clause 2, Article 10 of the Law on Data protects the continuity of data processing and governance, as well as the security of databases and information systems. The first group of conduct

consists of unlawfully obstructing or preventing data processing or governance. The second consists of attacking, appropriating, or destroying databases or information systems used for data management, processing, governance, and protection [5].

Obstruction or prevention may be carried out through technical or non-technical means. Technical measures include overwhelming a system, locking administrator accounts, interfering with connection protocols, deleting access keys, or disabling synchronization mechanisms. Non-technical measures may include intentionally withholding authentication credentials, unlawfully retaining storage media, preventing authorized personnel from accessing a system, or issuing false instructions to disrupt processing. The term "unlawfully" excludes temporary suspension, restriction, or blocking of access under a lawful decision made to protect a system, investigate an incident, or fulfill a legal obligation.

Attack, appropriation, and destruction reflect three different forms of interference. An attack seeks to bypass or weaken protective measures; appropriation seeks to obtain control over, or take possession of, data, databases, or administrator accounts; destruction seeks to damage, delete, encrypt, alter, or disable operations. A single act may contain several elements, such as infiltrating a system, encrypting a database, and demanding payment for restoration. Depending on the objective elements, consequences, and statutory prosecution thresholds, conduct that disrupts operations, deletes, damages, or alters data may be examined under Article 287 of the Criminal Code on the offense of obstructing or disrupting the operation of computer networks, telecommunications networks, or electronic devices. Where a subject bypasses warnings, access codes, or firewalls, or uses another person's administrative privileges to gain unauthorized access, seize control, interfere with functions, or steal, alter, or destroy data, Article 289 on unlawful intrusion into another person's computer network, telecommunications network, or electronic device may apply [10]. Article 10 of the Law on Data provides the basis for identifying prohibited conduct; criminal liability arises only where the criminal procedure authorities establish all constituent elements of the relevant offense.

The direct objects of protection under Clause 2 include the right to control data, data availability, and the continuous operation of data infrastructure. As public services, finance, healthcare, education, and logistics increasingly depend on real-time data, system disruption may produce cascading effects. The seriousness of the conduct therefore does not depend entirely on whether data are taken; preventing access or rendering data unavailable at a critical time may itself cause substantial harm.

3.3. Forging, intentionally falsifying, deleting, or damaging data in databases of the political system

Clause 3, Article 10 affords special protection to data in databases of Party and State agencies, the Vietnam Fatherland Front, and socio-political organizations [5]. Separate identification of this group of databases reflects the role of public-sector data in public administration, public-service delivery, policy formulation, determination of legal status, and the operation of the political system.

"Data forgery" means creating data or authentication indicators that cause non-existent data to appear legitimate. "Data falsification" means interfering with data so that their content no longer accurately reflects the original event, object, or status. "Data deletion" means causing data to cease to exist or become irretrievable, while "data damage" means impairing the readability, usability, verifiability, or interoperability of data. These four forms of conduct affect data in different ways, but all undermine the integrity and reliability of a database.

The seriousness of this group of conduct lies in the fact that data held by public authorities are often used as a basis for administrative decisions, budget disbursements, property registration, licensing, identity verification, or national statistics. Incorrectly altered data may lead to erroneous decisions; deleted data may delay procedures; and forged data may legitimize a non-existent entitlement. The harm extends beyond the agency administering the database to individuals and organizations that rely on the data to establish or exercise rights and obligations.

The provision uses the phrase "intentionally falsifying," but it remains unclear whether the requirement of intent also governs the acts of

deleting and damaging data. To ensure fairness and legal certainty in the attribution of liability, intentional interference must be distinguished from objective incidents, equipment or software failures, and professional errors lacking a harmful purpose. Such errors may still give rise to remedial obligations, disciplinary action, or other forms of liability, but should not automatically be equated with highly dangerous prohibited conduct. Where intentional falsification, deletion, or damage is carried out through system disruption or unlawful intrusion, Article 287 or Article 289 of the Criminal Code may be considered, as appropriate [10]. Data forgery, however, does not automatically fall within either offense; classification depends on the method, purpose, consequences, and satisfaction of all statutory elements. This issue should be clarified when sanctions and incident-verification procedures are developed.

3.4. Intentionally providing inaccurate data or failing to provide data as required by law

Clause 4, Article 10 prohibits two forms of conduct: intentionally providing inaccurate data and failing to provide data as required by law [5]. Unlike Clause 3, which concerns direct interference with data in databases of the political system, Clause 4 addresses the duty to provide data where such a duty is imposed by law. The provision helps ensure the quality, completeness, and timeliness of inputs into data-governance processes.

Providing inaccurate data means communicating or transferring data that the subject knows are factually incorrect, are incomplete in a manner that changes the substance of the information, have been unlawfully altered, or are outdated but are nevertheless represented as accurate. Intent is an important condition for distinguishing prohibited conduct from mistakes, measurement error, data-entry errors, or situations in which the subject has not yet received updated information. Assessment should consider the source of the data, verification procedures, prior warnings, the subject's capacity to identify the inaccuracy, and the response after the error was discovered.

Failure to provide data is prohibited only where a legal duty to provide such data exists. Before finding a violation, the competent authority must establish the legal basis for the request, the scope of the data, the obligated subject, the deadline and method of provision, and the subject's capacity to comply. Refusal to provide data because the request exceeds the authority's competence or conflicts with duties to protect state secrets, trade secrets, or personal data cannot automatically be treated as a violation. Likewise, force majeure or an objective technical impediment should be assessed differently from intentional concealment, delay, or non-cooperation.

Clause 4 plays an important role in data-driven governance. When data are connected and reused by multiple agencies, a single inaccurate source may generate numerous erroneous decisions in receiving systems. The principle of a single trusted data source, together with the standardization and synchronization requirements under Decree No. 278/2025/ND-CP, increases the responsibility of agencies that create, maintain, and provide master data [7]. The duty to provide data must therefore be accompanied by source-authentication mechanisms, records of update times, quality notifications, and prompt correction procedures.

3.5. Prohibited acts involving personal data and their relationship with Article 10 of the Law on Data

Article 7 of the Law on Personal Data Protection creates a specialized layer of protection for data associated with, or capable of identifying, a specific individual [8], [9]. Compared with Article 10 of the Law on Data, this protection focuses more directly on the lawfulness of processing, informational self-determination, privacy, and the risk of commodifying individuals through their data.

The first group includes processing personal data to infringe the State, national defense and security, public order and safety, or lawful rights and interests, as well as unlawfully processing personal data. This group overlaps partly with Clause 1, Article 10 of the Law on Data, but the Law on Personal Data Protection focuses on the legal conditions governing each processing activity, including purpose, legal basis, scope, duration, data-subject rights, and the responsibilities of controllers and processors.

The second group includes obstructing personal data protection activities and abusing such activities to violate the law. These provisions protect rights-enforcement and supervisory mechanisms, thereby preventing personal data protection from being invoked as a means of

concealing violations, obstructing investigations, or refusing lawful obligations. A legitimate exercise of the right to object, request erasure, or restrict processing must be distinguished from the intentional use of such procedures to destroy evidence or evade legal duties.

The third group includes using another person's personal data, or allowing another person to use one's own personal data, to commit unlawful acts; buying or selling personal data, except where otherwise provided by law; and appropriating, intentionally disclosing, or causing the loss of personal data. These acts directly infringe the data subject's control and security. Protection also extends to situations in which a person voluntarily lends a digital identity, account, or authentication information to another person for unlawful use; the fact that the data belong to the lender does not exclude legal liability.

The prohibition on buying and selling personal data must be interpreted consistently with the policy of developing a data market. The law does not prohibit every transaction involving data, but it does prohibit treating personal data as a commodity transferable independently of the rights and lawful control of the data subject, except where otherwise provided by law. Service provision, data transfers for a specified purpose and on a lawful basis, with rights-protection mechanisms and without creating a separate data repository for unrelated purposes, are not equivalent to buying and selling personal data [8], [9]. This distinction is important both for protecting privacy and for avoiding unnecessary restrictions on lawful data services.

4. LEGAL AND GOVERNANCE VALUE OF ESTABLISHING PROHIBITED ACTS

4.1. Protecting national interests, data security, and public order and safety

At the national level, the prohibitions affirm the direct relationship between data, sovereignty, security, and governance capacity. As state operations and essential infrastructure become increasingly dependent on databases, appropriating, destroying, falsifying, or disrupting data may have consequences comparable to disabling part of the physical infrastructure. Article 10 of the Law on Data enables early identification of dangerous conduct before its effects spread and provides a basis for coordination among data governance, cybersecurity, cyberinformation security, and protection of state secrets.

4.2. Protecting human rights, citizens' rights, and the lawful rights and interests of organizations

The prohibitions translate constitutional principles concerning private life, personal secrecy, honor, property, and access to information into specific behavioral limits. The Law on Personal Data Protection, in particular, confirms that data may not be processed merely because a technical actor has the capacity to collect or store them. Processing must have a lawful basis, pursue a proper purpose, remain within an appropriate scope, and respect the rights of the data subject. By prohibiting the buying, selling, appropriation, intentional disclosure, or unlawful use of personal data, the law protects privacy through both preventive and remedial mechanisms.

4.3. Ensuring the integrity, accuracy, availability, and reliability of data

The value of data depends on their quality and reliable usability. Inaccurate data circulated as correct may be more dangerous than the absence of data because they lead users to make erroneous decisions while creating an unwarranted sense of certainty. Prohibitions on forging, intentionally falsifying, deleting, damaging, or intentionally providing inaccurate data protect the integrity of the data chain from creation to exploitation. This integrity is a prerequisite for evidence-based governance, procedural automation, and data sharing across systems.

4.4. Strengthening the accountability of actors in the data ecosystem

A data activity commonly involves multiple actors: the creator, administrator, owner, controller, processor, infrastructure provider, intermediary, and user. Without clear limits, responsibility may be dispersed on the ground that an error originated in the system, the source data, or a third party. The prohibitions identify conduct that cannot be justified by internal arrangements or outsourcing. Any actor that directly performs, directs, authorizes, or knowingly participates in prohibited conduct must bear liability corresponding to its role and degree of fault.

4.5. Building trust in digital transformation and the data market

Developing data as a resource and an asset is sustainable only where parties trust that data have a lawful origin, are not arbitrarily altered or appropriated, and are used in a manner that respects the rights of relevant subjects. Prohibitions do not conflict with innovation; rather, they exclude business models based on unlawful data and reduce risk costs for compliant actors. International data-governance experience likewise emphasizes that broader access to and sharing of data must be accompanied by trust mechanisms and protection of rights and lawful interests [12].

5. ISSUES ARISING AND RECOMMENDATIONS FOR LEGAL IMPROVEMENT AND MORE EFFECTIVE ENFORCEMENT

5.1. Clarifying legal elements and criteria for determining fault

Guidance should be issued to interpret and identify open-textured concepts in Article 10 of the Law on Data, particularly "abuse," "infringe," "obstruct," "prevent," "appropriate," "destroy," "inaccurate data," and "failure to provide data." The criteria should be linked to access rights, purpose, method, type of data, degree of impact, foreseeability of consequences, and remedial measures. Greater specificity would reduce arbitrary application and assist enterprises and regulatory agencies in developing appropriate compliance procedures.

Fault requirements should also be clarified for each group of conduct. Clause 4 expressly refers to "intentionally providing inaccurate data," whereas Clause 2 and parts of Clause 3 do not fully distinguish intentional conduct from objective incidents, technical failures, or professional mistakes. Sanctions legislation should provide a mechanism for assessing fault on the basis of system logs, warnings received, the subject's authority, concealment, and conduct following the incident. A subject that promptly reports, isolates, restores, and cooperates in an investigation should be distinguished from one that intentionally deletes traces or continues to exploit the consequences.

5.2. Improving coordination in the application of law and the system of sanctions

A coordination mechanism should be established for the application of the Law on Data, the Law on Personal Data Protection, the Law on Cybersecurity, the Law on Cyberinformation Security, legislation on state secrets, and sector-specific laws. The mechanism should clearly identify the lead agency, jurisdiction, rules for transferring cases, safeguards against duplicate proceedings, and principles for determining which sector-specific law takes priority. Where an incident both exposes personal data and damages important data, a joint procedure is preferable to requiring organizations to submit separate reports to multiple authorities using different formats.

The prohibitions should also be aligned with the sanctions system. Prohibited acts do not all present the same degree of danger; sanctions should take into account the type and scale of data, the number of affected subjects, the consequences, benefits obtained, repetition, and cooperation in remediation. Where conduct shows signs of a criminal offense, files should be transferred promptly; where it does not reach the criminal threshold, administrative measures should be sufficiently deterrent and may include restoration orders, deletion of unlawfully obtained data, suspension of processing, or withdrawal of data products or services where necessary.

5.3. Strengthening mechanisms for proving data provenance, integrity, and traceability

Mechanisms for proving data provenance and integrity should be improved. Agencies and organizations managing important data, or data used for decisions with significant effects, should maintain immutable logs of creation, modification, access, sharing, and deletion; version-authentication mechanisms; information on sources and update times; change-approval procedures; and backup and restoration systems. These measures both prevent prohibited conduct and provide objective evidence when disputes or incidents occur.

5.4. Distinguishing lawful data transactions from prohibited trading in personal data

A clear distinction should be drawn between lawful data transactions and prohibited buying and selling of personal data. Guidance should specify the conditions applicable to data transfers, analytics services, sharing of de-identified data, transactions on data exchanges, and fee-based

arrangements. The core criteria should include purpose, legal basis, scope of processing, the possibility of re-identification, data-subject rights, and whether the recipient may create an independent data repository for separate purposes. Such clarity would protect personal data without eliminating the lawful data market.

5.5. Enhancing compliance capacity and public awareness

Compliance capacity and public awareness should be strengthened. State agencies and enterprises should adopt internal data-governance policies, least-privilege access controls, quality-assurance procedures, risk assessments, incident-response plans, staff training, and mechanisms for protecting whistleblowers. Individuals should be instructed not to lend accounts, identification information, or authentication data; to recognize unlawful collection practices; and to exercise rights of access, correction, erasure, and complaint. Prohibitions can operate effectively only where subjects understand the legal boundaries and have access to effective reporting channels.

6.CONCLUSION

Provisions on prohibited acts are a central component of Vietnam's legal framework for data. Article 10 of the 2024 Law on Data establishes four general boundaries designed to protect national interests, security and public order, the integrity and availability of data, databases, and information systems, and the lawful rights and interests of agencies, organizations, and individuals. Article 7 of the 2025 Law on Personal Data Protection adds a specialized layer of protection for privacy, informational self-determination, and the security of personal data.

The theoretical foundations of these provisions derive from the ease with which data can be copied, disseminated, combined, and used to amplify harm; asymmetries of power among actors; the need to reconcile public and private interests; and the importance of prevention before damage becomes irreversible. Their legal foundations are found in the Constitution, the Civil Code, the Law on Data, the Law on Personal Data Protection, cybersecurity and cyberinformation security legislation, and systems of administrative and criminal sanctions.

For the prohibitions to be effective in practice, Vietnam should further clarify the legal elements of each act, fault requirements, criteria distinguishing violations from technical errors, mechanisms for coordinating the application of relevant statutes, and measures for proving data provenance, integrity, and traceability. Such improvements would strengthen data protection and build the trust required for digital transformation, data sharing, and the responsible development of the data market.

7. ACKNOWLEDGMENTS

I would like to thank TNU- University of Sciences for supporting us to complete this article.

REFERENCES

[1] National Assembly of Vietnam, Constitution of the Socialist Republic of Vietnam, 2013.

[2] National Assembly of Vietnam, Civil Code No. 91/2015/QH13, dated 24 November 2015.

[3] National Assembly of Vietnam, Law on Cyberinformation Security No. 86/2015/QH13, dated 19 November 2015.

[4] National Assembly of Vietnam, Law on Cybersecurity No. 24/2018/QH14, dated 12 June 2018.

[5] National Assembly of Vietnam, Law on Data No. 60/2024/QH15, dated 30 November 2024.

[6] Government of Vietnam, Decree No. 165/2025/ND-CP dated 30 June 2025, detailing a number of provisions and measures for implementing the Law on Data.

[7] Government of Vietnam, Decree No. 278/2025/ND-CP dated 22 October 2025, on mandatory data connection and sharing among agencies within the political system.

[8] National Assembly of Vietnam, Law on Personal Data Protection No. 91/2025/QH15.

[9] Government of Vietnam, Decree No. 356/2025/ND-CP dated 31 December 2025, detailing a number of provisions and measures for implementing the Law on Personal Data Protection.

[10] National Assembly of Vietnam, Criminal Code No. 100/2015/QH13 dated 27 November 2015, as amended and supplemented by Law No.

12/2017/QH14, Law No. 59/2024/QH15, and Law No. 86/2025/QH15.

[11] Hanoi Law University, Textbook on General Theory of the State and Law, Justice Publishing House, Hanoi, 2023.

[12] OECD, Recommendation of the Council on Enhancing Access to and Sharing of Data, OECD/LEGAL/0463, adopted 6 October 2021.