Page 1409 - 1430 **DOI:** *https://doij.org/10.10000/IJLMH.113908*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 6

2022

Protecting Personal Data Pursuant to the Vietnamese Law: Regulations, Appraisal and Recommendations

DR. PHAM HONG HANH[1]

ABSTRACT

The 2013 Constitution of Vietnam upholds human and basic rights and obligations of citizens in which personal data protection is one of the most important human rights-related issues. Although it has been recognized in many different documents, so far, a complete and comprehensive legal framework has not been enacted to separately regulate personal data protection. The absence of a complete legal framework directly affects the effectiveness in protecting personal data in particular and protecting privacy in general in Vietnam. The limitations in the provisions of Vietnamese law on the protection of personal data will be highlighted within the scope of this study. With such purpose, the study mainly uses analytical methods to evaluate the current provisions of Vietnamese law on personal data protection. In addition, legal comparison method will be also applied to suggest some comprehensive regulations for Vietnamese laws on personal privacy protection following the practical examples of other nations.

Keywords: *Personal data, personal data process, information safety.*

I. INTRODUCTION

In the era of digital technology, especially with the strong development of breakthrough technologies in the 4.0 industrial revolution, protecting personal data is becoming more urgent than ever. Personal data is considered as an endless input and value for the digital economy. Most industries and fields take advantage of personal data use for data processing such as administrative, medical, criminal, civil status, nationality, authentication, e-commerce, education, finance, banking, tax and tax operations, information technology, communication, artificial intelligence, Internet of Things, Cloud Computing, Big Data, Fast Data. Therefore, the proper use of personal information to minimize the violation of personal information is extremely important.

Vietnam is one of the countries with the highest speed of Internet development and application in the world with the number of more than 64 million users, accounting for more than two thirds

[1] Author is a Doctor Lecturer at Faculty of International Law, Hanoi Law University, Vietnam.

 [ISSN 2581-5369]

of the population (66%), an increase of more than 19% compared to 2018, ranking 13th in the world in terms of users, including 58 million Facebook accounts, 62 million Google accounts[2].

The more technology application level is applied, the greater the provision and use of personal information will be. The situation of disclosure, leakage, theft, trading of personal data is common in cyberspace. More and more personal data is subjectively collected, analyzed and processed for different purposes without notifying customers or they let illegal acts happen to occur. Some typical cases are : VNG Company's disclosure of more than 163 million customer accounts; The Gioi Di Dong and Dien May Xanh Company exposed more than 5 million emails; and tens of thousands of payment card information such as Visa and credit cards of customers; hackers attacked the server system of Vietnam Airlines, uploaded the Internet with 411,000 member customer accounts of the Golden Lotus program; the fatct that customer information is disclosured by Vietnamese taxi service brokers to invite customers via SMS; Customer data of FPT Company is publicly posted online[3].

(A) Need of the study

In Vietnam, the protection of personal data is scattered in many different documents which can be divided into two groups:

First, documents with provisions on personal data in general, specifically: (1) The Civil Code recognizes the protection of privacy, personal secrets and family secret; (2) The Law on Cyber Information Security recognizes the rights of information subjects for organizations and individuals processing information, responsibilities and obligations of the party that collects and processes personal data; (3) The Law on Information Technology stipulates the conditions for collection and processing and use other people's personal information on the internet; the right of the information to the people who stores his or her personal information in the network environment and responsibility of the people that collects, processes and uses others' personal information. (4) The Cybersecurity Law regulates prohibited acts in cyberspace, invasion of individual's privacy, also stipulates the responsibilities of the information system owner in implementing management and technical measures to prevent, detect any acts of cyber espionage, infringing on state, business, personal and family secrets on such information system. Then, the in-charge authorities promptly remove information related to violated behavior. They also coordinate and fulfill the requirements of the specialized network security force on cyber espionage prevention and combat to protect information belonging to state, work,

[2] Ministry of Public Security (2019), Proposal for the development of a Decree on Personal Data Protection.
[3] Ministry of Public Security (2019), Report on the proposal to develop a Decree on Personal Data Protection

business, personal, family and private life on the information system

Second, documents with regulations on protection of personal data in specialized fields, specifically: The Law on Medical Examination and Treatment stipulates the protection of records, health and medical information; The Law on Tax Administration provides the protection of financial secrecy in terms of income and tax payment; The Law on Credit Institutions provides the protection of account confidentiality and account transactions; The Law on Insurance Business stipulates the protection of confidentiality for insurance contracts; The Law on Social Insurance provides the protection of secrets and against illegal access to insurance data; The Law on Electronic Transactions stipulates the principles of information security of the parties involved in electronic transactions.

Although it is recorded in many different texts; however, the legal provisions on personal data protection are inadequate and unable to form an effective legal basis in preventing and properly handling violations of personal data.

For the above reasons, there is need to evaluate the limitations in the provisions of Vietnamese law on the protection of personal data and give some recommendations to complete these regulations.

(B) Objective of the study

The study was carried out to meet the following objectives:

- To examine provisions of the current Vietnamese law on the protection of personal data
- To evaluate the limitation in the provisions of the current legislation on the protection of personal data such as lack of detail, contradiction between regulations, lack of completeness, incompatible with reality.
- To propose some suggestions to improve the Vietnamese legal framework on personal data protection.

(C) Methodology

The article uses a combination of different research methods such as analytic-synthetic method, comparative law method and so on to achieve research objectives. For example, analytical and synthesis methods are used to review the provisions of Vietnamese law on the protection of personal data. The comparative law method is used to provide a solution for Vietnam to complete the regulations on the protection of personal data.

II. OVERVIEW OF VIETNAMESE LAW ON PERSONAL DATA PROTECTION

(A) General principles of personal data protection

Personal data protection is part of the right to privacy (*Right to Privacy*). Article 21 of the 2013 Constitution stipulates the right to privacy as follows:

"*1. Everyone has an inalienable right to privacy, personal and family secrets and the right to protect their honor and reputation. Information on private life, personal and family secrets are protected by law.*

2. Everyone has the right to keep their correspondence, phone calls, and telegrams confidential and other forms of private communication. No one shall illegally open, control or seize the correspondence, telephone, telegrams and other forms of communication of private information."

In addition, this right is also recognized in many other relevant documents, specifically:

The 2015 Civil Code stipulates that "*1. Private life, personal and family secrets are inviolable and protected by law; 4. Letters, telephones, telegrams, electronic databases and other forms of private exchange of personal information are guaranteed to be safe and confidential. The contract must not disclose information about each other's private lives, personal and family secrets which known in the course of contract establishment and performance without other's permission.*"[4]

The 2018 Cybersecurity Law prohibits the use of cyberspace to violate the laws on national security, social order and safety, post or disseminate information in cyberspace with contents that infringe on state or business secrets, personal, family and private life in cyberspace[5].

In particular, in relation to personal data, the Cybersecurity Law prohibits the use of cyberspace for: a) Dispossessing, trading, seizing, intentionally disclosing information belonging to personal and family secrets, and private life that can affect the honor, reputation, dignity, rights and legitimate interests of individuals; b) Deliberately deleting, damaging, misplacing, changing information, personal, family secrets, and private lives that are transmitted and stored in cyberspace; c) Intentionally changing, canceling the built-in technical measure that applied to protect information of family secrets and private life; d) Posting on cyberspace information of personal, family secrets and private life that is contrary to law; đ) Deliberately listening, recording, and illegally camcording conversations; e) Other acts intentionally infringing upon

[4] Article 38 Civil Code 2015
[5] Article 8 Law on Cybersecurity 2018

 [ISSN 2581-5369]

personal, family secrets and private life[6].

The Law on Cyberinformation Security 2015 affirms the principle "organizations and individuals must not infringe the network information security of other organizations and individuals". Specifically, organizations and individuals must not illegally access, use, disclose, interrupt, modify or destroy information systems of other organizations or individuals. Handling network information security incidents must ensure by the lawful rights and interests of organizations and individuals, without infringing on private life, personal secrets, family secrets of individuals, private information of organizations [7].

At the same time, the Law also prohibits the illegal collection, use, distribution and trading of other people's personal information; take advantage of loopholes and weaknesses in information systems to collect and exploit personal information, prohibit illegal infiltration of cryptographic secrets and lawfully encrypted information of agencies, organizations and individuals[8].

In addition, the Law on Information Technology, the Law on Telecommunications, the Law on Post also recognizes privacy protection, personal information protection and strict prohibited acts of infringing upon privacy in postal, telecommunications, and network information security activities. The 2009 Law on Medical Examination and Containment stipulates on protecting the confidentiality of citizens' records, health and medical information[9], The Tax Administration Law 2019 regulates the protection of financial secrets of citizens' income and tax payment[10], the Law on Credit Institutions regulates the protection of the confidentiality of citizens' accounts and account transactions

The Criminal Code has dedicated a chapter on crimes of infringing upon human freedom, civil liberties and democracy (Chapter XV) and corresponding penalties such as trespassing on other people's residences[11], crime of infringing upon the confidentiality or security of another's

[6] Article 17 Law on Cybersecurity 2018
[7] Article 4 Law on Cyberinformation Security 2015
[8] Article 7 Law on Cyberinformation Security 2015
[9] The right to confidential information about health status and private life that documented in the medical record belongs to patients. This information is only allowed to be released with the patient's consent or to share information and experiences to improve the quality of patients' diagnosis, care and treatment or in other cases prescribed by law (Article 8 Medical examination and treatment). Medical examination and treatment practitioners are obliged to keep confidential the patient's medical condition, the information that the patient has provided and the medical record, except for other cases prescribed by law (Article 37 of the Law on Medical Examination and Treatment)
[10] Taxpayers are entitled to keep information confidential, except for information that must be provided to competent state agencies or public tax information as prescribed by law (Clause 4, Article 16 of the Tax Administration Law 2019). Tax administration agencies have the duty to keep taxpayers' information confidential, except for information provided to competent authorities or publicly disclosed as prescribed by law (Clause 4, Article 18 of the Law on Tax Administration).
[11] Article 158 of the Criminal Code

correspondence, telephone, telegram or other form of private information exchange[12]. The Criminal Procedure Code affirms that no one may illegally infringe upon his/her residence, private life, personal and family secrets, secure and confidential correspondence, telephone, telegraph and other forms of private communication[13]. Such Code reconfirmed specific regulations on the searching, seizure of mail, telephone, telegram, electronic data and other forms of private communication[14]. It also prescribed the application of investigative and procedural measures such as audio recording, secret video recording, secret phone call, secret electronic data collection[15]; application authority [16]; application period [17]. The Law on Access to Information 2016 also stipulates on handling inaccurate information disclosed by state agencies[18].

(B) Conditions for collecting, processing and using personal data

The Civil Code 2015 recognizes principled regulations in the collection, storage and use of personal data. Accordingly: *The collection, storage, use and disclosure of information relating to private life and personal secrets must be consented. The collection, storage, use and disclosure of information related to family secrets must be agreed upon by family members,*

[12] Article 159 of the Criminal Code

[13] Article 12 Criminal Procedure Code 2015

[14] The seizure of electronic means and data shall be carried out by competent authority to conduct legal proceedings and people with related expertise to participate. In case they cannot be seized, they must be backed up to storage media and confiscated as evidence (Article 196 of the Criminal Procedure Code).

[15] After prosecuting the case, during the investigation, the authority conducting the procedure may apply special investigation and procedure measures such as: sound recording, secret video recording; answer the phone secretly; confidential collection of electronic data. A special investigative and procedural measure may be applied to the following cases: Crimes of infringing upon national security, drug-related crimes, corruption-related crimes, terrorism-related crimes, money-laundering crimes; Other organized crimes of particularly serious crimes Article 223, Article 224 of the Criminal Procedure Code.

[16] 1. The head of the provincial-level investigating agency, the head of the military-regional-level military investigating agency or higher shall personally or at the request of the Chief Procurator of the provincial-level People's Procuracy, the Chief Procurator of the Military Procuracy of the military zone shall have the right to issue a decision on the application of special investigation and procedural measures.

2. If the case is handled by the district-level investigating agency or regional military investigation agency, Heads of district-level investigating agencies and regional military investigating agencies shall request heads of provincial-level investigating bodies and heads of military-zone-level military investigation agencies to consider and decide on application.

3. The decision to apply special procedural investigation measures must be approved by the chief procurator of the same level of procuracy before execution. The head of the investigating agency that has issued the application decision is responsible for closely examining the application of this measure, and promptly requesting the procuracies to cancel it if deems it no longer necessary.

4. Heads of investigating bodies, heads of competent procuracies and enforcers of decisions on application of special investigative procedures must keep secrets Article 225 of the Criminal Procedure Code.

[17] The time limit for application of special investigative and procedural measures shall not exceed 2 months from the date of approval by the Procurator General. Complicated cases may be extended but not exceeding the time limit for investigation as prescribed in this Code Article 226 of the Criminal Procedure Code.

[18] In case a citizen believes that the public information is inaccurate, he/she shall propose to the agency that has made the information public. Within 15 days from the date of the petition, that agency is responsible for checking the accuracy of information and respond to citizens; If it is determined that public information is inaccurate, it must promptly correct and disclose the corrected information. Incorrect public information in any form must be corrected in that form (Article 22).

 [ISSN 2581-5369]

unless the law has other provisions. The opening, controlling and seizure of people's correspondence, telephone, telegram, electronic databases and other forms of private information exchange shall be carried out only in cases prescribed by law.[19]

The Law on Cyberinformation Security only stipulates the general conditions under which the data processor can: a) Collect personal information after the consent of the person on the scope, the purpose for which such information is collected and used; b) Personal information is only collected for purposes other than the original purpose after the consent of the person; and c) Do not provide, share, or distribute personal information that are collected, accessed, or controlled to third parties. except for the case with the consent of that person or at the request of a competent state agency[20].

At the same time, according to the provisions of the Law on Information Technology 2006, organizations and individuals that "collect, process and use personal information of others in network environment must be agreed by that person, unless otherwise provided by law." Exceptions for the collection, processing and use of personal information without consent appear when such personal information is used for the following purposes: a) Signing, modifying or performing contracts for the use of information, products and services in the network environment; b) Calculating prices and charges for using information, products and services in the network environment; c) Performing other obligations as prescribed by law.[21]

Resolution No. 27/NQ-CP of the Government dated 7/3/2022 on approving construction documents of personal data protection has documented the following five cases where personal data is processed without people's consent, including:

- The processing is crucial in response to an emergency that threatens life, health or safety of the person or others. The data controller, the data processor, the third Party are responsible for proving such case:
- The disclosure of personal data in accordance with the law;
- The processing is necessary because of national defense and security requirements which is carried out by competent authorities as prescribed by other laws;
- Competent state agencies to investigate and handle law violations in accordance with provisions;
- Personal data is processed by a competent state agency for the purpose of serving the

[19] Article 38 Civil Code 2015.
[20] Article 17 Law on Cyberinformation Security
[21] Clause 3, Article 21- Law on Information Technology 2006

 [ISSN 2581-5369]

operation of the state agency in accordance with the provisions of law.[22]

a. Personal rights of the data

- According to the provisions of the Cyberinformation Security Law, people have the right to:
- Requesting organizations or individuals that process personal information to provide theirs that such organizations and individuals have collected and stored. [23]
- Requesting organizations and individuals processing personal information to update, modify or cancel their personal information that the organization or individual has collected, stored or stopped providing their personal information to third parties[24].

Besides, the Law on Information Technology also recognizes the right of individuals to request organizations and individuals to store personal information on the network to check, the person has the right to claim compensation for damages caused by violations in the provision of personal information[25] (Article 22).

b. Responsibilities and obligations of the Party that collects and processes Personal Data

Article 46 of the Law on Electronic Transactions 2005 provides the general principles under which *"1. Agencies, organizations and individuals are obligated to choose security measures in accordance with the provisions of law when conducting e-transactions.*

2. Agencies, organizations and individuals are not allowed to use, provide or disclose information about private life or information of other agencies, organizations and individuals that they accessed to or controlled in electronic transactions without their consent, unless otherwise provided by law."

The Law on Information Technology also recognizes responsibilities of person who collects, processes and uses personal information of others, including: "*a) Inform the form, scope, location and purpose of the collection, processing and use of his or her personal information; b) Use the collected personal information for the right purposes and only store such information*

[22] Article 1 Resolution No. 27/NQ-CP dated 7/3/22 approving the dossier to develop the Decree on protection of personal data
[23] Article 17, Clause 3 - Law on Cyberinformation Security
[24] Article 18, Clause 1 - Law on Cyberinformation Security
[25] Article 22 Law on Information Technology

 [ISSN 2581-5369]

for a certain period of time in accordance with the provisions of law or as agreed between the two parties; c) Take necessary technical and management measures to ensure the availability without being stolen, disclosed, altered or destroyed; d) Immediately take necessary measures upon receipt of a request for re-inspection, correction or cancellation as prescribed in Clause 1, Article 22 of this Law; Do not provide or use relevant personal information until it is corrected" [26]

In addition, the Law on Cyber Information Security also has a number of similar provisions and more specific about the responsibilities and obligations of the party that collects and processes personal data. Specifically:

- Agencies, organizations and individuals participating in cyberinformation security activities shall have to coordinate with competent state agencies and other organizations and individuals in ensuring cyberinformation security [27];
- Agencies, organizations and individuals that process personal information are responsible for ensuring cyberinformation security for the handling information. They must develop and publicly announce measures to handle and protect personal information of their organizations and individuals. [28]
- Obligation not to provide, share, or distribute personal information that are collected, accessed, and controlled to a third party, except with the consent of that person or at the request of a competent state agency. [29]
- Make requests and notify the person with information or provide him his personal information with access to self-update, amend, cancel; notify him in the event that the request cannot be fulfilled due to technical factors or other factors when receiving a request from the person to update, amend, cancel personal information or request to stop providing personal information to third parties. Organizations and individuals that process personal information must destroy stored personal information as soon as the purposes are completed or expire the storage period and notify such person.

Organizations and individuals that process personal data must delete stored personal information when the purposes are completed or expire the storage period and notify the related person. [30]

[26] Article 21 Law on Information Technology
[27] Clause 1, Article 15 of Law on Cyberinformation Security
[28] Article 16 Law on Cyberinformation Security
[29] Article 17 Law on Cyberinformation Security
[30] Clause 2, Clause 3, Article 18 of the Law on Cyberinformation Security

 [ISSN 2581-5369]

Management measures and appropriate techniques must be applied by organizations and individuals that process personal information. In order to protect personal information collected and stored, they must also comply with standards and technical regulations on network information security assurance. [31]

c. Violation processes

Depending on the nature, seriousness and consequences of the violation, violations of regulations on personal data protection will be subject to the following violation forms

First, civil liability, including compensation for person who is in breach of personal data.

Second, currently the sanctioning of administrative violations in personal data infringing activities is mainly recorded in Decree No. 98/2020/ND-CP which regulated on sanctioning of administrative violations in commercial activities, production and counterfeit and prohibited trading and protect consumer rights. Decree No. 15/2020/ND-CP provides penalties for administrative violations in the fields of post, telecommunications, radio frequency, information technology and electronic trading. Following these documents, violations of regulations on the protection of personal data such as violations of regulations on collection and use of personal information; violations of regulations on updating, modifying and canceling personal information, ensuring the safety of personal information online; violations of regulations on storage, rental, transmission, supply, information access, collection, processing, exchange and use; violation of consumer information protection will be fined from 10,000,000 VND to 70,000,000 VND. At the same time, such violations may be subject to additional penalties including forced destruction of personal information.

Third, criminal liability. The 2015 Criminal Code stipulates two crimes related to the act of violating personal data. Specifically, depending on the nature and seriousness of the violations, offenders of "Infringing upon the confidentiality or security of correspondence, telephones, telegrams" or another form of communication of another's private information." will be subject to a fine of from 1 million to 20 million dong, non-custodial rehabilitation from 1 year to 2 years or imprisonment from 3 months to 2 years. In addition, offenders may be banned from holding certain posts from 1 to 5 years.[32] Offenders who "illegally give or use information on computer networks, telecommunications networks, and the Internet" shall be fined from VND 30,000,000 to VND 1,000,000,000, non-custodial reform for up to 3 years, or imprisonment from 6 months

[31] Clause 1, Article 19 of the Law on Cyberinformation Security

[32] Article 125 Criminal Code 2015

 [ISSN 2581-5369]

to 7 years. In addition, they may be banned from holding certain positions, practicing certain professions or doing certain jobs for 1 to 5 years. [33]

III. EVALUATION OF THE CURRENT PROVISIONS OF VIETNAMESE LAW RELATED TO THE PROTECTION OF PERSONAL DATA

First, regulations on the protection of personal data are scattered, lack of concentration. Currently, there is no separate legal document regulating personal data. On the contrary, the issue of protection of personal data is found in many different documents that lead to overlaps and contradictions. This can be illustrated with the regulations on management competence in the field of personal data protection and administrative penalties for violations of regulations on personal data. Specifically,

- Regarding management authority

According to current regulations, The Ministry of Information and Communications is the agency in charge of coordination and management of cyberinformation security [34] while the Ministry of Public Security is the agency in charge of network security management [35]. However, according to the provisions of the Law on Cyberinformation Security and the Law on Cybersecurity, the two areas of management of these two agencies actually overlap. Specifically, network security under the provisions of the Law on Cybersecurity is "the assurance that activities in cyberspace is not detrimental to national security, social order and safety, legitimate rights and interests of agencies, organizations and individuals." [36] Network information security according to the provisions of the Law on Cyberinformation Security means "protection of information, systems on the internet from being accessed, used, disclosed, interrupted, modified or unauthorized destruction to ensure the integrity, confidentiality and availability of information." [37] With this definition, activities to ensure network information security are in fact to ensure network security. Since the purpose of protecting information online is the prohibition of access, use, disclosure, interruption, modification or unauthorized destruction to ensure integrity and confidentiality and information availability. To ensure that activities in cyberspace do not cause harm to national security, social order and safety, and lawful interests of agencies, organizations and individuals. In other words, activities within the scope of network information security assurance coordinated and managed by the Ministry of

[33] Article 288 Criminal Code 2015
[34] Article 52 of the Law on Cyberinformation Security
[35] Article 36 of the Law on Cybersecurity
[36] Clause 1, Article 2 of the Law on Cybersecurity
[37] Clause 1, Article 3 of the Law on Cyberinformation Security

Information and Communications are also found in the scope of activities of the network security assurance by the Ministry of Public Security. However, there is only a clause in the Cybersecurity stipulating the responsibility of coordination between the Ministry of Information and Communications and the Ministry of Public Security and Ministry of National Defense in protecting network security [38] without specifying the scope or content of coordination.

- Regarding handling of administrative violations.

According to Article 46 of Decree No. 98/2020/ND-CP on sanctioning administrative violations in commercial activities, production and trading of counterfeit and prohibited goods and protection of consumer rights, the act of transferring consumer information to a third party without the consent of the consumer in accordance with regulations, unless otherwise provided by law, will be fined from 10,000,000 VND to 20,000,000 VND. Double fines will be applied if the relevant information is the consumer's personal confidential information. According to Article 84 of Decree No. 15/2020/ND-CP, the act of providing or sharing or disseminating personal information collected, accessed, controlled to third parties without the consent of the owner of personal information shall be fined from 20,000,000 VND to 30,000,000 VND. On the other hand, Decree No. 15/2020/ND-CP stipulates that additional penalty for the violation is applied. This is the forced requirement of destruction of personal information while Decree No. 98/2020/ND-CP does not stipulate. In essence, telecommunications service users are also consumers. They are specifically consumers of telecommunications services. However, the fine for those who illegally transfer personal information of telecommunications service consumers in these two regulations are different. If as provided for in these two decrees, such regulations refer to the act of transferring personal information to a third party without the consent of that person in the field of post, telecommunications, information technology, electronic transactions which are only applied measures to force destruction of personal information due to violations.

Second, there is no unified concept of “personal data”. Current legal documents are using various terms such as “personal information”, “private information”, “confidential information”, “consumer information”, “private life”, “personal secrets”…without specific definitions for all of the above terms except for the definition of “personal information”. Despite the first mention of the term “personal data” in Resolution No. 27/2022 of the Government dated March 7, 2022 on the approval of the dossier for the formulation of the Decree on Personal Data Protection, they have not yet given a definition of "personal data".

[38] Article 38 Law on Cybersecurity

 [ISSN 2581-5369]

This leads to duplication and difficulties in practical application [39]. For example, can consumer's product usage habits be considered as personal data? Is accessing and handling "privacy secrets" or "personal secrets" different from "personal information"? In particular, the concept of "personal information" in a number of current legal documents is not equivalent to the concept of "personal data" compare to the approach of other countries in the world. Decree No. 72/2013/ND-CP (amended and supplemented by Decree 27/2018/ND-CP on the management, provision and use of Internet services and information on the network) provides that personal information is *"information associated with identification, personal identity including name, age, address, identity card number, phone number, email address and other information as prescribed by law*"[40]. While Cyberinformation Security Law defines that "personal information" means "information associated with the identification of a particular person"[41].

Compared to the definition of "personal data" in the EU law and other nations, current definition of Vietnamese law on "personal information" narrower than the concept of "personal data" as approached by many other countries. Namely, *General Data Protection Regulation* - GDPR of the European Union defines personal data as "all information relating to a natural person directly or indirectly identified or identifiable."[42] Similarly, Singapore Personal Data Protection Act 2012 defines personal data as "data of a person, whether true or not, is personally identifiable from that data or personally identifiable from that data and in combination with other information that the organization has access to." [43] According to these regulations, if the information does not include the individual's name, but that information, in combination with others can be personally identifiable, it is considered personal data. Contrary to the provisions of the Law on Cyber Information Security as well as Decree No. 72/2013/ND-CP, only information through which an individual is identified can be considered personal information.

Third, there are no regulations on transferring personal data of Vietnamese citizens abroad. Vietnamese citizens' data is being illegally transferred abroad. Most domestic and foreign service providers collect personal data of Vietnamese citizens. They conduct analysis and processes to create new data for economic purposes. Some businesses store this data overseas

[39] Ministry of Public Security, Report "Preliminary impact assessment of some contents proposed to develop a Decree on protection of personal data"
[40] Clause 16, Article 3 of Decree 27/2018/ND-CP on management, provision and use of Internet services and online information.
[41] Clause 15, Article 3 of Law on Cyberinformation Security.
[42] Article 4 Regulation 2016/679 of the Parliament and the Council of 27 April 2016 on the protection of personal data in relation to the processing of personal data and the free movement of data, and repeal the No. 95/46/EC (Personal Data Regulation)
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
[43] Section 2, Part I of the Singapore Personal Data Protection Act.

without registration, failure to comply with the provisions of the law, leading to the situation of disclosure or acts causing material and spiritual harm to agencies, organizations and individual.[44] However, there is currently no regulation on the transfer of personal data abroad, such as the conditions for transfer, cooperation between the competent authority of Vietnam and that of the foreign country in the protection of illegally transferred personal data. Although there is a provision regarding international cooperation in cyberinformation security and cyber security Law, the regulation briefly noted the international cooperation in prevention and control acts of violating the law on network security and cyberinformation security as one of the contents of international cooperation in this field [45].

Fourth, existing legal provisions governing actions affecting personal data are not adequate. Specifically, Law on Cyberinformation Security, Law on Cybersecurity, Law on E-Transactions as well as other specialized laws regulate the collection, storage, provision, sharing practices, distribute or destroy, purchase, sell or transfer to third parties. In fact, there are other behaviors affecting personal data but they have not been regulated by laws such as analysis, encryption, access permission or decrypt data. For instance, mobile apps require users to agree with its permissions such as camera monitoring, contacts, memory access rights, then can such application be used to collect personal information or the case of businesses when selling or providing the services, they already asked for customer's personal information. The business then keeps this information to form a personal data store and analyze those types of data for the sake of business.

In addition, the following personal data processing after the person with the data died has not been specified in any current documents, such as who can agree to get for access, the retention period of the data owner's personal data upon death.

Fifth, the regulations of conditions for processing personal data are not specific. Current regulations on conditions for collecting and processing personal data recorded only one content: "the consent of the person with information, unless otherwise provided for by law". This regulation is vague without clarifying some of the following basic issues:

- How can it be considered if the person has consented to the collection and processing of its information? For example, answering sale-man questions about first and last name, phone number, address, date of birth, preferences, shopping habits is considered as the consent for the business to store, publish or analyze

[44] Ministry of Public Security, Report "Preliminary impact assessment of some contents proposed to develop a Decree on protection of personal data"
[45] Article 7 of the Law on Cybersecurity, Article 6 of the Law on Cyberinformation Security.

 [ISSN 2581-5369]

personal information? In case the silence of the subject of information is considered as his/ her agreement for another to process his/her personal information?

- The form of agreement of the person. For instance, if the person only gives consent to another subject verbally to process personal data without recorded evidence, will it be considered consent? When there is a dispute, the burden of proof of consent lies with either party, the data processor or the data subject;
- If the data subject is satisfied, the consent of the data subject is considered valid. In order to avoid the data processor intentionally does not provide information or intentionally mislead data subjects related to information processing activities to obtain consent from data subjects;
- The case of processing personal data without the consent of the data subject. Although Resolution No. 27/2022 has recorded some cases processing personal data without the consent of the subject, what activities can affect personal data without the subject's consent? Whether all activities affect personal data is possible without the consent of the data subject;
- Other issues such as how long the data subject's consent is considered valid? Could data subjects withdraw consent? Are there any conditions attached to the withdrawal of consent?
- Provisions on sanctions for violations of the law for violations of the law on protection of personal data.

Sixth, regulations on sanctions for violations of the law on protection of personal data are not specific or un appropriate to reality.

- The provisions on criminal prosecution for violations of the law on protection of personal data

As mentioned above, currently the Criminal Code 2015 stipulates two crimes related to personal data including: "*Infringement of confidentiality or security of correspondence, phone calls, telegram or other form of private communication." (Article 159) and "Crime of illegally giving or using information on computer networks or telecommunications networks" (Article 288).* However, these two crimes are not specified, they directly related to the ongoing violations of the law regarding personal data. On the other hand, the punishment prescribed for these two crimes is not commensurate with the reality and consequences of current private information

 [ISSN 2581-5369]

infringement acts. For example, the unauthorized intrusion and interference into the electronic information system with malicious code to collect private information is taking place seriously in the network environment. Especially when public concerned about the spread of the Covid-19 epidemic, notices and instructions on epidemic prevention from authorities, health organizations, hackers have increasingly forged notifications to spread malware and perform phishing attacks.

In 2020 alone, hundreds of billions of dong were appropriated by hackers through banking-related cyberattacks, in which are mainly cases of stealing OTP of users' transactions. The main way of hackers is to trick users into installing spyware to steal OTP code, then process illegal transactions. On average, BKAV monitoring system has detected more than 15,000 spy-software on mobile phones every month. A typical example is the case of VN84App, a software to collect OTP messages from banking transactions that appropriated up to billions VND by infecting thousands of smartphones in Vietnam[46]. However, the punishment for this behavior is served to the maximum of a year. In case of aggravating circumstances, such as organized crime, repeated crimes, causing serious consequences or recidivism, the maximum penalty is only two years in prison or re-offend, the maximum penalty is two years imprisonment.[47]

- For regulations on handling administrative violations

Although the current law on handling administrative violations, there are already provisions for a number of violations related to the protection of personal data, the above regulations are not fully and comprehensively guaranteed to serve as a basis for sanctioning violations that are not in fields such as postal, telecommunications, information technology, radio frequency, commerce, manufacturing, trading in counterfeit and banned goods, protecting consumer rights.[48] Examples of intentional disclosure of personal data related to the adoption process for the purpose of profiteering such as personal information of children who need to find a replacement family (including full name; date of birth; gender; ethnicity; place of birth; health status; full name, name of birth parent or guardian, foster facility, address, contact phone number of the child care facility). There is no legal basis for sanctioning administrative violations due to the inability to apply Decree No. 98/2020/ND-CP on penalties for administrative violations in commercial activities, production and trading of counterfeit and banned goods and protect consumer rights. The same situation with Decree No. 15/2020/ND-

[46] https://nhandan.vn/thong-tin-so/toan-canh-an-ninh-mang-viet-nam-nam-2020-ton-that-hon-1-ty-usd-do-virus-may-tinh-632235/, accessed April 30, 2022.
[47] Article 125 Criminal Code 2015
[48] Ministry of Public Security, Report "Preliminary impact assessment of some contents proposed to develop a Decree on protection of personal data"

CP stipulating penalties for administrative violations in the fields of post, telecommunications, radio frequencies, information technology and electronic transactions. In addition, the current administrative penalty for violations of personal data protection is inappropriate. Specifically, according to the provisions of Decree No. 15/2020/ND-CP, the highest administrative sanction is 70 million VND.[49] If compared with the fines specified in EU law, or some other countries, such amount of fine is low. It can be failed to achieve the purpose of preventing or adequately punishing violations. For example, under GDPR, the maximum fine can be up to 20,000 EUR or 4% of the total annual revenue worldwide of the previous fiscal year, the higher option is applied accordingly.[50] Also, as specified in the Personal Data Protection Act of Singapore, the maximum fine for an organization violation is $1 million, while that for an individual is $200,000.[51]

- **Some recommendations**

First, promulgating specialized legal documents on the protection of personal data to overcome the current scattered, lack of focus, this will be the general document regarding personal data, protection of personal data, processing of personal data and responsibilities of agencies and organizations in protecting personal data; overlapping provisions in other legal documents will be abolished.

Second, to clarify the concept of personal data in the same way as many countries around the world.

That is the regulation of personal data in the direction of "personal information and through such information or in combination with other information, can be individually identifiable". Such regulation will ensure the information, though it is not possible to directly identify an individual, when it is collected, aggregated, and combined with other information can help to identify a particular individual on psychological, economic status, political ideology which is also considered personal data to be protected by law. In addition, it is necessary to identify what types of personal data are sensitive ones to provide a higher level of protection.

Third, fully identify behaviors affecting personal data that is considered "data processing", add behaviors that are not currently mentioned such as data analysis, decoding, and encryption to ensure effective protection of personal data before any factors can affect this type of property. Specific regulations on conditions, contents and obligations of organizations and individuals

[49] Clause 5, Article 102 of Decree No. 15/2020/ND-CP stipulating penalties for administrative violations in the fields of post, telecommunications, radio frequencies, information technology and electronic transactions.
[50] Clause 5, Article 83 GDPR.
[51] Article 48J of the Law on Protection of Personal Data.

when processing personal data, especially children and sensitive data, processing personal data after the data subject's death.

Fourth, specific regulations on subject data such as the right to have decision making power to authorize to a third party to process his/her data; the right to be informed as soon as the data is to be analyzed; the right to make a request to the data processor to end the personal data processing, or the right to let others to access, delete or remove collected personal data; the right to make complaints, to claim compensation in case of a breach… For such issue, there should be specific provisions on the content related to the "consent" of the data subject such as conditions for the consent to be valid (purposes, types of personal data that can be processed, transferred, shared to a third party, the behavioral and awareness competence of data subject at the time making decision and such decision should be made upon voluntary basis); form of consent (E.g. consent must be in writing or in other clear, understandable and accessible forms and can be proved); the valid period of the consent; the withdrawal of consent ; the obligation to prove consent in the event of a dispute; cases and conditions for which personal data is processed without the consent of the data subject (e.g. for the interests, national security, social order and safety; in cases where it is specified by law as an emergency, a life-threatening danger or seriously affect the health of data subjects or public health; serve investigation and handle of illegal acts, etc.).

Fifth, supplementing regulations on the movement of personal data beyond national borders such as delivery and licensing conditions, coordination between the competent authorities of Vietnam and these of foreign countries involved in handling violations, protecting data that have been illegally transferred.

Sixth, establishing a specialized agency for the protection of personal data. This agency is in charge of protecting the interests of data subjects, preventing any misuse of personal data, ensuring the compliance with the provisions of the law and promoting awareness of data protection; receiving registration dossiers for cross-border transfer of personal data; receive complaints about personal data breach, at the same time, propose the Ministry of Public Security (the agency responsible for chairing and coordinating in ensuring network security) to handle violations, handle complaints about personal data protection, decide whether to agree or disagree with the application for the processing of sensitive personal data, registration dossiers for cross-border transfer of personal data, make decisions to stop processing personal data.

Seventh, adjust sanctions for violations of the law on protection of personal data. Specifically:

- For regulations on criminal prosecution, supplement provisions on criminal

 [ISSN 2581-5369]

sanctions related to regulations on protection of personal data such as setting up a system to collect information and personal data on a large scale, against the law; build spyware that collects personal information and data; large-scale personal data trading; unlawfully disclose personal data that causes damage to life, property. At the same time, specific instructions on criminal composition for two crimes currently are regulated in the Criminal Code, specifically "*Infringing upon the confidentiality or security of another's correspondence, telephone, telegram or other form of private communication"* (Article 159), *"Crime of illegally giving or using information on computer networks or telecommunications networks"* (Article 288) and consider increasing penalties for these two crimes.

- For regulations on administrative handle. In order to have a legal basis for handling personal data breaches, it is necessary to replace the current regulations related to the handling of violations of personal data in Decree No. 98/2020 and Decree No. 15/2020 with comprehensive adjustment regulations for violations such as acts of violating regulations on the rights of data subjects regarding the processing of personal data, violation of the data subject's consent to personal data, violation of regulations on processing personal data after the death of the data subject, violation of regulations on notifying data subjects about personal data processing, violation of regulations on handling personal data without consent of data subject. The higher level needs to be charged, at the same time stipulating a fine equivalent to a certain percentage (E.g. 2% or 4%) of the total profit of the organization/individual from the breach of personal data. In each specific case, the violation handling agency will consider which penalty to apply.

IV. CONCLUSION

In such a rapidly developing information technology era, invasion of personal data is becoming more common, in which there are mainly three types of violations, including: buying and selling personal data, disclosing personal information in newspapers, social networks and unlawfully collect information. There are many reasons for this situation in which, one of the most crucial one is the incomplete legal provisions on the protection of personal data. There is no concept of "personal data", some of personal data violations have not been identified, or regulations on penalties for violations are not appropriate with consequences… With a scattered number of current legal documents regarding certain matters of personal data, the enactment of a separate

legislation on the protection of personal data is necessary for a complete legal framework. Therefore, in the near future, a law on protection of personal data should be introduced, specifically: *First*, clarify the concept of personal data, sensitive personal data; *Second*, concretize the rights of data subjects; *Third*, specify obligations and responsibilities of subjects related to data processing and responsible for personal data protection; *Fourth*, adjust regulations on handling personal data violations to ensure compliance with practice and consequences.

*****

 [ISSN 2581-5369]

V. REFERENCES

- Ministry of Public Security, Report "Preliminary impact assessment of some contents proposed to develop Decree on protection of personal data" (2019)
- Ministry of Public Security, Report on requesting the development of a Decree on Personal Data Protection (2019)
- Ministry of Public Security, Report on the actual situation of personal data protection, (2019)
- Vietnam, 2013 Constitution
- Vietnam, 2015 Civil Code No. 91/2015/QH13
- Vietnam, 2015 Criminal Code No. 100/2015/QH13
- Vietnam, Criminal Procedure Code 2015 No. 101/2015/QH13
- Vietnam, Law on Cyberinformation Security 2015 No. 86/2015/QH13
- Vietnam, Law on Cybersecurity 2018 No. 24/2018/QH14
- Vietnam, Law on Information Technology 2006 No. 67/2006/QH11
- Vietnam, Law on Electronic Transactions 2005 No. 51/2005/QH11
- Vietnam, Government Resolution No. 27/NQ-CP on approving the dossier for the formulation of the Decree on Personal Data Protection.
- Vietnam, Government Decree No. 98/2020/ND-CP dated August 26, 2020 stipulating penalties for administrative violations in commercial activities, production and trading of counterfeit and banned goods and protection of human rights consumption.
- Vietnam, Government Decree No. 15/2020/ND-CP dated February 3, 2020 provided penalties for administrative violations in the fields of post, telecommunications, radio frequencies, information technology and electricity transactions death.
- Nguyen Van Cuong,“ Current status of the law on personal information protection in Vietnam and directions for improvement” (2020), Journal of Legislative Research, No. 15 (415)
- Chu Thi Hoa, *Report on reviewing the law on protection of personal data in Vietnam, Documents at the Workshop within the framework of the 2020 program of activities of the project "Strengthening the law and justice in Vietnam", organized by the Ministry of Industry and Trade. Security coordinated with the United Nations Development*

 [ISSN 2581-5369]

Program to be held in Hanoi on January 9, 2020.

- China, Law on Cybersecurity 2016
- Singapore, Law on Protection of Personal Data 2012.
- China, Law on Protection of Personal Data 2021
- Nguyen Huong Ly, Vietnam's current laws on data protection, personal information and privacy https://nacis.gov.vn/nghien-cuu-trao-doi/-/view-content/214123/phap-luat-hien-hanh-cua-viet-nam-ve-bao-ve-du-lieu-thong-tin-ca-nhan-va-quyen-rieng-tu
- Regulation 2016/679 of the Parliament and the Council of 27 April 2016 on the protection of personal data relating to the processing of personal data and the freedom of movement of data, and repeals Regulation 95/. 46/EC (Personal Data Regulation):https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
- 22. Tran Thi Thu Phuong, "General Regulations of the European Union on Personal Data Protection and Some Recommendations to the National Assembly, Government and Vietnamese Enterprises", (2021) Legislative Research Journal, No. 23 (447)

*****