VNU Journal of Science: Legal Studies, Vol. 39, No. 1 (2023) 30-44

Original Article

Addressing the Challenges of Data Privacy Protection Law in Vietnam

Bach Thi Nha Nam*, Nguyen Ngoc Phuong Hong

University of Economics and Law, Vietnam National University Ho Chi Minh City, No. 669, Highway 1, Quarter 3, Linh Xuan, Thu Duc, Ho Chi Minh, Vietnam.

Received 6 December 2021
Revised 08 March 2022; Accepted 20 June 2022

Abstract: Frontier-less nature of the Internet not only enables the free flow of data across countries, but also brings new challenges including risks to privacy. For personal data protection, the rules are set out in Vietnam's Civil Code 2015 and in multiple sectorial laws. Recently, in order to enhance the best effort in protecting personal data, Vietnam updated its legislative agenda and planned to enact an initial Decree on Personal Data Protection drafted by the Vietnamese Ministry of Public Security after its first issuance in 2019. This article presents the journey to establish the right recognition, focuses on analysing the current legislation in protecting personal data, and challenges to effective protection of the right to data protection in Vietnam such as technological advancement in information technology, a need to balance between technology modernisation and public security, the effect of Asian values debate and Confucianism. A conclusion is drawn from the challenges and the remedies discussed, with great emphasis being laid upon modifying the data protection law as the suitable trend for the Vietnamese legal framework.

Keywords: Privacy, data protection, Vietnam.

* Corresponding author.
E-mail address: nambachnha@gmail.com
https://doi.org/10.25073/2588-1167/vnuls.4413

1. A Long Journey of Recognition of Data Privacy Protection in Vietnam Since the Mid- twentieth Century

1.1. Recognition of the Right to Privacy

In general, data privacy protection is concerned with guaranteeing the proper processing (gathering, use, and storage) of personal data by both public (government) and private (business) organisations. However, debates regarding what data protection is, why data protection is important, and how data protection is implemented have persisted throughout Vietnam's legislative history. Before any data protection law could be promulgated in Vietnam, the country had to establish the right to privacy as the first step toward personal data protection. Under Vietnam's first constitution in 1946, the right to privacy was mentioned as an inalienable right stipulated in Article 11, stating that no one may intrude on the privacy of Vietnamese individuals' homes or correspondence. This is an initial recognition of personal information from the State.

Under succeeding constitutions in the years including 1959, 1980, 1992, the right to privacy has been legally recognised and protected although the wordings and content are more or less the same. Individuals' right to privacy recognised in the newest version of the Constitution in 2013 was broadened and more closely to the international standards protecting human rights.

Unlike previous versions of constitutions, Vietnam opened the right holder of the privacy right to not only a citizen right, but also a human right. Article 21 of the 2013 Constitution states: “Everyone has the right to inviolability of private life, personal secrets and family secrets; and has the right to protect his or her honour and reputation. The security of information about private life, personal secrets or family secrets shall be guaranteed by law. Everyone has the right to privacy of correspondence, telephone conversations, telegrams and other forms of private communication. No one may illegally break into, control or seize another’s correspondence, telephone conversations, telegrams or other forms of private communication”.

It is of note that, in the period from 1954 to 1980, when the north of Vietnam was completely liberated, embarking on socialist-oriented economic construction, the State promulgated Law No. 103 - SL/ L.005 on guaranteeing the Physical Liberty and the Inalienable Rights with respect to houses, objects, or correspondence of citizens in 1957. This law clearly states: "The people's right to freedom of body and inviolability to housing, objects and mailing are respected and guaranteed. No one shall infringe upon these rights". In addition, Article 16 of the law also clearly stipulates sanctions for violations of the right to personal information: "Those who arrest, detain, search people, search objects, houses and correspondence in contravention of this Law may, depending on the case, be administratively disciplined or be fined from 15 days to 3 years in prison. If commit torture and use corporal punishment, this one will be further punished according to common criminal law”.

After the liberation of the South and the reunification of the country in 1975, Vietnam was in the process of revising and integrating its legal system. During the time, national security and public order took precedence over the protection of human rights and fundamental rights, such as the right to privacy and the right to personal information protection. Legislative history from the 1980 Constitution to before 1986 shows that the law-making mainly focused on the state apparatus organisation field. It explains why the regulation on the protection of personal information was not really widespread at this time. After 1980, when Vietnam joined many international treaties on human rights, notably the 1966 International Covenant on Civil and Political Rights - ICCPR in1982, it set the requirements the compatibility of domestic rules on the right to privacy and the right to personal information protection with the Convention. Later, the 1985 Criminal Code

provided sanctions for violations related to privacy, such as the provision in Article 120 about the crime of infringing upon citizens' residences, Article 121 about the crime of infringing upon other's privacy or safety of correspondence, telephone and telegraph. The versions of 1946, 1959, 1980 Vietnam Constitution stipulated the privacy of correspondence and residence information. The 1985 Criminal Code also dealt with the privacy of correspondence and the residence personal information whereas other contents in the concept of personal information were still left behind.

Overall, the protection of personal information in Vietnam before 1986 was recognised in principle, while the concept, subject's rights and obligations, the scope, procedures, etc. have not been regulated, and criminal sanctions for dealing with infringement on personal information are just for residence and correspondence only [1]. Hence, personal information which is legally recognised in the legal framework in Vietnam has emerged since the mid-twentieth century after the accidents of intricate and unpredictable disclosure and leakage of data, the increased presence of hostile forces in the cyberspace environment, and among the endeavour to fight against the hostile forces and hackers in the cyberspace.

1.2. The Development of Data Privacy Concept and Legislation for the Cyberspace in Vietnam

At the premiere of the 21st century, Vietnam witnessed an internet outbreak with almost 17.3 million internet users in Vietnam in 2006, increasing 17 million in comparison with 2000 [2]. Since 2006, Vietnam has steadily improved data privacy safeguards in e-commerce and consumer legislation to eventually reach the level of the OECD Guidelines (or APEC Framework) in 2014 [3]. On 29/11/2005, Law No. 51/2005/QH11 on e-transactions was promulgated. With the issuance of Civil Code 2005, Civil Procedure Code 2005 as well as specific laws like Commercial Law 2005, Law on Information Technology 2006, Correspondence Law 2010, Telecommunications Law 2009, Publication Law 2005, HIV/AIDS Prevention and Control Law 2006, Law on Protection of Consumers' Rights 2010, Decree No. 52/2013/ND-CP on e-commerce etc, the regulations of privacy protection, consumer confidentiality, Internet users' rights and responsibilities, procedure, forms, methods as well as subjects accountable for the protection of personal information have all been established into the Vietnamese legal regime.

At the same time, these legal documents highlighted the need to preserve some sensitive subjects' personal information (e.g. children, HIV-infected people, patients, postal service users, telecommunications service users and subscribers etc.), as well as prohibited including citing information or providing or disclosing information without user's consent. Personal information processing, collection, and usage have also been regulated, however, the notion of personal information processing has not been clarified. In 2009, the infringement on personal information was expanded and clarified in criminal law. Specifically, Articles 226, 226a, 226b have added some provisions about the crime of illegally using the information in computer networks (Articles 226), illegally accessing computer networks, telecommunications networks, the internet or digital devices of other persons (Articles 226a) and using computer networks, telecommunications networks, internet or digital devices to appropriate property (Articles 226b) with a maximum fine up to VND 200,000,000, a prison term up to 15 years or life imprisonment (in aggravating circumstances).

Keep up with the substance of Article 37 of the 2005 Civil Code, the 2015 Civil Code states that "If a piece of information negatively impacting a person's honour, dignity, or prestige is put on a means of mass media, that piece of information should be deleted or

rectified by that sort of means. If that piece of information is kept by an agency, organisation or individual, such entity is required to cancel it. In case it is impossible to identify the individual who provided the information that jeopardises a person's honour, dignity, and/or prominence, the latter person has the right to request a court to declare that such piece of information is incorrect".

Besides, the right to private life, personal secrets and family secrets is also regulated in Article 38 under the 2015 Civil Code: "The private life, personal secrets and family secrets of a person are inviolable and protected by law. The collection, preservation, use and publication of information about the private life of an individual must have the consent of that person; the collection, preservation, use and publication of information about the secrets of family must have the consent of all family's members, unless otherwise prescribed by law. The safety of mails, telephones, telegrams, other forms of electronic information of an individual shall be ensured and kept confidential". This laid the groundwork for the approval of the Law on Cyber-Information Security in November 2015 as a result of a long-term plan and substantial effort. The Law on Cyber-Information Security, like mentioned legal documents, requires the owner's consent before personal data processing (including collection, modification, use, storing, providing, sharing, or transmitting), and stipulates that organisations and individuals handling personal data are responsible for information security and must publish their own privacy policies. It is the first time Vietnam has defined the "processing" of personal information and mentioned the wider definitions for personal information under the law. With the issuance of this law, the content of data privacy protection in Vietnam is generally more precise and stronger [4]. Vietnam continued to strengthen the government's capacity to regulate the flow of information and secure key information infrastructure by requiring businesses providing services on Vietnam cyberspace to notify users directly if their data is breached, damaged, or lost in the Law on Cybersecurity promulgated in 2018. The Cybersecurity Law reflected numerous parallels with China's Cybersecurity Law in enhancing the role of government in controlling the security in the Internet and the flow of information [5].

Despite the fact that the right to privacy and personal secrets is a constitutional right, except the protection of the security of the cyber information, Vietnam does not currently have a unified piece of data protection law. Alternatively, rules and regulations on privacy may be found in a variety of legislation. Nowaday, Vietnam's legal privacy safeguards are growing, including a set of privacy principles in the Consumer Protection Law and more comprehensive principles in e-commerce legislation. It can be said that the most detailed data privacy protections in Vietnam are found in e-commerce and consumer sectors [6].

In reality, the implementation of legal documents will be determined by each instance. Enterprises in the banking and finance, education, and healthcare sectors may be subject to particular legal provisions. For example, Decree No. 117/2018/ND-CP dated September 11, 2018 provides the protection of confidentiality and provision of client informations: "A credit institution or foreign bank's branch shall only provide client information to other organisations or individuals in one of the following cases: i) Other organisations or individuals having the right to request the credit institution or foreign bank's branch to provide client information are specified in codes, laws and resolutions of the National Assembly and ii) The client's consent granted in writing or other forms under the agreement with the client is available". State agencies in the fields of audit, tax, police, judgment enforcement, customs, courts, procuracies, and their competent persons are specifically listed in Article 10 of the decree as having the right to request the credit institution or foreign bank's branch to provide client information.

Recently, the Ministry of Public Security (MPS) issued a draft Decree on Personal Data Protection in February 2021 and called for public comments. This is the first run through Vietnam that proposes to establish a far-reaching data protection law, this regulation is expected to apply to "offices, associations and people identified with individual information", with certain exemptions [7]. Under a preliminary assessment, the Decree incorporates a significant number of the necessities of the EU Data Protection Directive 1995, including some limits on automated processing, data minimisation, sensitive data protection, export limits based on the law of the recipient countries, and individual admittance to the courts. This Decree is expected to enhance the legal protection of data privacy in Vietnam.

Although the recognition and perfection of data privacy protection in Vietnam's legal regime have been a long journey in the coming time, it is no doubt that the recognition of the right to privacy is the backstage for the promulgation of data privacy protection Under the strong impact of the widespread legislation of data protection law in the region and in the world, Vietnam cannot be in the exempt domain against the trend.

Moreover, the GDPR has set the best model for the legislation of data protection law around the world and in the Southeast Asian region. Consequently, Vietnam has still evaluated the legal tradition and the cultural values in the perception of the data protection law from other jurisdictions and found by itself the suitable values for its law-making evolution of the right to privacy and personal data protection law.

2. Closer Look at Vietnam's Draft Decree on Personal Data Protection

In Vietnam, a general constitutional protection for privacy, or a civil action or criminal accusation of infringement of privacy is the legal remedies which are sufficient enough to develop the comprehensive data protection law against the background. Data protection rules can also be found in the sectoral law, covering most aspects of the operation in the private sector such as protecting consumers, e-commerce, electronic transactions, publication, press, credit reports or medical reports.

Vietnam's domestic law provides a set of basic data privacy principles, to the international standards at least approximating the minimum provided for by the OECD Guidelines or Council of Europe Convention 108. In particular, Vietnam has since 2006 gradually developed a range of data privacy protections in its e-commerce and consumer laws, to the level of the OECD Guidelines (or APEC Framework) by 2014 [3]. Since the 2016 Law on Cyber Information Security (CISL), a highest-level law enacted by the National Assembly, expanded existing scattering protections into the single most detailed set of data privacy principles, but with its scope limited to commercial processing and only in cyberspace [3].

Under state surveillance, the Law on Cybersecurity 2018 has focused on regulating cyber activities that impact national security and social order and safety. However, except the legally recognised general principles, data privacy legal regime which covers the national public sectors is far from the demand. Such protection is sometimes by different legislation in principles and enforcement mechanisms from that covering the private sector.

Among recent efforts to promulgate the comprehensive law of data protection beyond cyberspace and covering the public sector, the draft Decree on Personal Data Protection by MPS has reflected the reach of such aims. As a Decree made by the Government, it will not be made by the National Assembly, and therefore does not have the highest legislative status as a law, contrasting with the CISL issued before. With personal data protection becoming such a prominent issue in recent years, the draft is a necessary step in bringing Vietnam's domestic regulations up to international standards, and

offers some welcome additions and changes to the existing regulations.

2.1. Scope of Application

The scope of the law is comprehensive, stating that it applies to agencies, organisations and individuals related to personal data (Art. 1), with some exceptions. Hence, its application covers the public sector and the private sector. The scope of the law extends to anyone "doing business in Vietnam" (Art. 4.2), not only those located in Vietnam. It is unclear in some provisions if the text applies only to the data of Vietnamese citizens.

Other definitions are also expansive. "Personal data processor", the key party to determining the scope of the law, "means an agency, organisation or individual at home and abroad that performs personal data processing activities" (Art. 2.8). The definition of personal data processors includes both domestic and foreign entities, but it is not clear how many of the provisions of the decree will apply to them. Data controllers, and those who do processing for them, are both referred to as "processors" (art. 2.8), and others who receive personal data are "third parties" (Art. 2.9). Personal data is defined conventionally in terms of identifiability (Art. 2.1), "data about individuals or relating to the identification or ability to identify a particular individual", divided into "basic" personal data, and "sensitive" personal data.

2.2 Registration of Sensitive Data Processing

"Sensitive" data is given a very extensive definition (Art. 2.3) including most usual categories: political and religious opinions, health data, sexual orientation, genetic and biometric data, as well as gender status and location data. It is noted that the list included both gender identification and sexual orientation, it possibly shows a sign of the government's moving towards more liberal attitudes about such issues. Also included are categories that are potentially very broad, namely "personal financial data", "personal data about social relationships" and "other personal data as specified by law to… need necessary security measures".

Sensitive personal data is treated with separate rules for its processing and sharing. Sensitive personal data must be registered with the Personal Data Protection Committee - PDPC located within the MPS (Art. 20), by an application requiring extensive information about the proposed processing and its legal basis. It must be accompanied by an impact assessment report which will assess the potential harm to data subjects and set out measures to deal with such potential harm. The PDPC is to process applications within 20 days of receiving a valid application.

The regulation is under the criticism that all private sector processors will process sensitive data including its employee data, which may incur significant costs in terms of time, money, and human resources, but it is highly doubtful that the PDPC would have sufficient resources to process the expected volume of applications within the specified timeline [7]. Although there exists some exceptions to the registration requirements, almost are applicable to public sector bodies (involving crime, health care, social security, judicial functions, statistics etc.) (Art. 20.4).

2.3. Principles and Rights of Data Owners

Eight key principles of data protection are stated briefly (Art. 3), among which definition of legitimate purposes are not specified except the general language "personal data is collected only in cases where it is necessary by law". The principles set out do not amount to specific rights and obligations in the subsequent articles in the whole decree.

Those who are the originators of personal data have specified rights. Those rights include the following:

- To allow or not allow personal data processors or third parties to process their personal data;
- To receive notices from the personal data processors at the time of processing or as soon as possible;

- To request the personal data processors to correct, view, and provide a copy of their personal data;
- To request the personal data processors to terminate the processing of personal data, restrict the right to access personal data, terminate the disclosure or access to personal data, delete or close collected personal data;
- To file complaints in specified circumstances;
- To claim compensation in the case of a breach.

Most of these rights can be infringed if there exist other legal provisions disallowing, or limiting them in some way. A waive of these rights can be applied through the data owner's consent and ignored upon request from in various situations of public interest, emergencies, for statistics or research after de-identification, and where according to the provisions of law (Art. 10). The exception is subject to the public concern that the rule may be abused widely by the government's executive branch, especially ministries by granting them de-facto ability to interpret laws and regulations by using circulars and executive decisions while no legitimate interest exceptions are specified to allow such processing.

In GDPR, legitimate interest is the most flexible of the GDPR's lawful bases for processing personal data. Theoretically, "Interests" can refer to almost anything here, including an organisation (public or private) or a third party's commercial interests or wider societal benefits. In general, the condition applies when:

- The processing isn't required by law, but there's a clear benefit to it;
- There is little risk of the processing infringing on data subjects' privacy; and
- The data subject should reasonably expect their data to be used in that way.

Taking a look at a specific example of a type of processing that is considered a legitimate interest under the GDPR [8]: An organisation is looking into the way it stores job applicants' personal details. It is legally required to store this information for six months, however, the organisation decides it wants to retain the data for longer than this, because it foresees scenarios where an applicant wasn't right for the role being advertised, but they might be suitable for a future position. In this case, the organisation is entitled to hold on to personal details under the legitimate interest condition, and keep personal data beneficial for both the applicant and the organisation.

It seems legitimate interests are the most appropriate lawful basis for all data processing activities, however the legitimate interest is the lack of legislation in the Vietnamese draft degree.

2.4. Cross-Border Transfer of Personal Data

The personal data of Vietnamese citizens must be kept within the borders of Vietnam. The personal data of Vietnamese citizens can only be transferred upon the satisfaction of the following four conditions:

- The data owner's consent is granted for the transfer;
- The original data is stored in Vietnam;
- The proof is obtained that the recipient country, territory or a specific area within the recipient country or territory has issued regulations on personal data protection at a level equal to or higher than that specified by the draft decree;
- Written approval is obtained from the PDPC.

The draft decree then proceeds to obviate this requirement and says that transfer may be made upon obtaining consent from the personal data owners and the making of a commitment to protect that data. The article seems not clear about the satisfaction of the required conditions.

Vietnam enacted Law on Cyber Security (CSL) in 2018 introducing the controversial control of data localisation requirements, imposing severe penalties on the publication of anything considered to be anti-state activities, which some commentators considered "imposes tremendous obligations on both onshore and, especially, offshore companies providing online services to customers in Vietnam" although

CSL did not prevent data stored in Vietnam from being transferred overseas [9].

Vietnam currently requires overseas data transfer under the consent or government approval and The PDPC is supposed to complete processing within 20 working days (Art. 21.8), the processor must store data transferred, consents etc, for three years (Art. 21.4), the PDPC will evaluate each data transfer regime annually (Art. 21.5).

It can be seen that the draft Decree raised big concerns for the private organisations to overcome the administrative and financial barriers including increasing cost, time, and human resources across many industries. For example, in the common sectors such as e-commerce, banking, travel, education, health care, etc, there are a tremendous demand to transfer personal data overseas, they usually process such data in a selected country outside of Vietnam or use cloud services with physical servers located outside of Vietnam. The draft Decree requests that all companies sending personal data overseas have to store data in Vietnam, it would create huge costs. Additionally, the PDPC's approval would unavoidably delay transactions and data transfers.

2.5. Data Protection Authority

The draft Decree creates PDPC comprised of no more than 06 comrades, working part-time, appointed by the government. Its Chairman is the Director of the MPS Department of Cyber Security and High Tech Crime Prevention and Control (Art. 23).

In many jurisdictions, PDPC is a separate and specialised data protection body, which can investigate and make findings against the private sector, then and its role and function, operation should be independent from any unnecessary influence including public authority. However, the suggestion of the PDPC in the draft Decree seems to describe the "Ministry model" of data protection, still adopted in China and Taiwan [10].

Vietnam should be expected to learn the independent model in the European countries or some other countries in the region to establish a specialised data privacy body, and separate its responsibilities for enforcement different from a diffuse array of sectoral ministries and telecommunications authorities.

2.6. Other Issues

This draft Decree does not unambiguously include a data breach notification requirement for companies as covered by the CSL 2018, requiring prompt notification of data breaches to the Cybersecurity department of the MPS, and for companies to notify users directly of such breaches. The draft Decree stipulates the obligation to promptly notify PDPC of violations related to personal data protection activities (Ar. 28.3). Companies must therefore still comply with multiple regulations besides the Decree.

The draft Decree stipulates the fine level specifically. Violations of the draft decree will receive impressive fines of from 50 to 80 million VND for a first offense. Violations related to sensitive personal data, cross-border transfer of personal data, and second offences of other violations will receive a fine of from 80 to 100 million VND. And additional repeats of the specified offences will receive a fine of 5% of the revenue of the entity that has been obtained in Vietnam.

The draft Decree also covers other issues as well. It addresses the processing of children's data, data of deceased individuals, obligations of the data processors, etc.

The draft Decree on personal data protection shows a move in the awareness among the public and the authority, and significant efforts of legislators toward global standards. Overall, Vietnam's draft Decree, if enacted, would constitute a strengthening of its data privacy legal regime. To some extent, it offers clarification to previously confusing regulations although in others proceeds to increase that confusion.

Even though the draft Decree shows the similarities of the EU Data Protection Directive 1995, including some limits on automated

processing, data minimisation, sensitive data protection, and export limits based on the law of the recipient country, it also reflects the influences of the GDPR in the inclusion of genetic and biometric data in sensitive data, and fines based on business turnover [10]. What the current draft poses big concerns is the independence of the PDPC, a body belonging to MPS under the Government in its power over the approval of processing sensitive data, and over personal data exports, and the potential barriers for the foreign companies.

3. Challenges Vietnam Facing in Lifting from State Surveillance to Approaching Personal Data Protection

3.1. The Effect of Asian Values Debate and Confucianism

Despite the fact that the Universal Declaration of Human Rights (UDHR) was approved by the United Nations' 56 members in 1948, there is no Asian regional convention on human rights. That is the reason why, when European countries began to attach human rights concerns to economic and trade agreements, some Asian countries resisted this pressure by “Asian values debate”.

Some leaders, notably Lee Kuan Yew of Singapore and Mahathir Mohamad of Malaysia, promoted the idea of “Asian values” as an explanation and justification for distinctive Asian cultural and political systems [11], meaning that Asian people preferred being governed by soft authoritarian, collectivist oriented states rather than the individualist, liberal democratic structures advocated by the West [12] and "individuals must put the state's rights before their own” (The spokesman of China's Foreign Ministry in 1993 World Conference on Human Rights in Vienna). It is reasonable to say so in someway because of the absence of freedom-oriented perspectives in Asian tradition.

Conventionally, the phrase ”Asian values" has been associated mostly with Confucian teachings, with Buddhist and Taoist legacies. Indeed, under the effect of Confucianism, Asian people have believed in the mission of sacrificing one's own for the common welfare, which is a mindset naturally admitted by the public.

Civic virtue “gongmindaode”, defined as people' dedication to the common good of their community even the sacrifice of their private interests, is believed as the primary motivator for public achievement [13]. Similarly, Confucius provides a clear point to the fact that the two pillars of the imagined edifice of Asian values, namely loyalty to family and obedience to the state [14]. In the concept of human rights and fundamental right, until the 20th century, “data privacy”, or “personal information” still seemed a “Western’ notion” in Asia. That is the reason why the ASEAN Human Rights Declaration, the first regional declaration in Asia concerning data privacy, containing specific references to personal data including privacy protection was not passed until 2012. Nowadays, in many Asian countries, privacy is a constitutional right and recognised as a human right.

Belonged to Eastern Asia culture, Vietnam is a country influenced by Confucianism and full of village nature. People are encouraged to be supportive, helpful and love each other. In other words, Vietnamese people not only live as individuals but also as part of their families and villages. Private life is often considered as not important as the public. In addition to legal regulation, one of the most significant instruments for successfully regulating social interactions and adjusting each individual's conduct in Vietnam is public opinion, including moral standards. People argue that an act considered unethical to society, customs or habits will not only affect that individual, but also destroy the image of the family, clan, and romantic community. Therefore, it is necessary for the family members to watch the others, parent to monitor their children, husband and wife to surveillance their partner, etc.

In general, each Vietnamese individual is not only held accountable for his/her actions

before the law but moral judgment also. Furthermore, in a long period of warfighting for independence, people are warned about espionage and enemy commandos from invading, including habits such as paying attention to the activities and lives of those around them, which formed a special caring and curiosity about others' life [15]. Social values and Vietnamese traditional mindsets certainly have overshadowed the importance of privacy protection and the need to perfect the legal framework relating to data privacy protection in Vietnam.

3.2. The Conflict Between State Surveillance and Privacy Protection

There is always a conflict between state surveillance and privacy protection around the world. However, because of historical features of a prolonged war, especially after the reunification in 1975, Vietnam defined the urgent duty of revising and building state organs as well as the legal system. At this time, as long as keeping the peace and rebuilding the country, tough policies and strict state control in all aspects are established. For the sake of the state's interest and public order, authorities and groups such as the Youth Union, the Women's Union, the neighbourhood group etc sometimes were prying too far into the private lives of families and individuals.

Surveillance of personal information to ensure national security is still prevalent until now, especially in the context of urgent national issues such as patient tracing during the covid pandemic, protecting national political security, etc.

Most concerns focus on the attempt of the state to exercise massive and constant surveillance over cyberspace to police the online population and its vague language to give almost blanket authority to punish any netizens at the state's discretion [16]. Another strategy employed is hiring opinion influencers and online commentators to follow political blogs and social networking sites to engage in online battles against hostile forces. The coercive measures mostly invite resistance from the Internet users and the hired commentators do not have the capacity to provide persuasion of argument on rational grounds. It also invited a negative effect to the younger generation into underground forums fostering daily activity exceeding 10,000 unique users or more on the deep and dark web [17].

The Vietnamese government's recent censorship legislation requires social media companies to maintain local offices in Vietnam and store local user data within the country under the CSL 2018. If a company provides services on the Internet or on a telecommunications network or provides other value-added services on the Internet to customers in Vietnam, and collects, exploits, analyses and processes personal data, customer information or any information created by customers in Vietnam, the company will be required to store the personal data created by customers within Vietnam, in Vietnam, for a period to be specified by the Government. Offshore companies affected by this requirement will be required to establish a branch or representative office in Vietnam.

Even cloud space must reside on a device or system that is both physical and tangible (e.g., data centres or server farms) [18]. In an effort to scrub any trace of critical or "toxic" speech online, to counteract negative views and fake news, especially those that are hostile to the Vietnamese Government, the state continued mandating companies to remove content, and suspended online newspapers [17].

On the one hand, the state's rigorous control and surveillance of personal information ensure national security, but on the other hand, it is the potential to violate each person's privacy.

For example, measures undertaken to fight and protect against COVID-19 have given rise to significant legal implications for the rights and freedoms of individuals. Discussions and controversies focused on several topics such as the processing of health data by public authorities; the data protection requirements needed to be met by trustworthy and efficient

apps; the tracing of location data; as well as data subjects' rights in connection with states of emergency in Vietnam. Tech experts are expressing concern over how the masses of data collected will impact the privacy of users in the rolling out of the contact-tracing app Bluezone. For example, the contact history data is often kind of anonymised, but the current app asks users to enter a phone number, this means the server can map the data to a phone number, and from there to an actual person, the server can tell whom you met, when and for how long although the developer team states that they only use the data for contact-tracing, and only authorised health authorities are allowed access [19].

Based on the observations from the GDPR, it allows for the processing of sensitive data when this is necessary for reasons of public interest in the area of public health, such as protecting against serious threats to health. The framework developed by the EU Commission provides that tracing apps must be voluntary, transparent, temporary, cyber secure, use temporary and pseudonymised data, and should rely on Bluetooth technology, and be approved by national health authorities [20].

It has been stressed that the right to the protection of personal data is not an absolute right, it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. The situation in Vietnam is riddled with the problems of the technology of pseudonymised data, and strong commitments to the legitimate processing of personal data in the lack of specified and detailed legal principles such as the principle of proportionality as in the GDPR.

3.3. Dilemma in Technology Modernization Without Stifling Control and Public Security

Given the adoption of the LCS, other relevant law relating to privacy protection and the direction which the draft Decree have taken, the question is whether Vietnam can find a proper way between developing cyberspace, information technology and their functions in e-commerce, e-government and moderating the negative effects to the individual privacy life, private companies with Vietnamese customers, especially multinational companies.

On the one hand, Vietnam wants to speed up the modernisation of its internet by pushing for the adoption and implementation of cloud computing. The development without stifling control shall touch every facet of life in Vietnam, by such, the Government is highly supportive.

On the other hand, Vietnam is trying to keep its essential management in scrupulously watching and shaping developments. The greatest obstacle is probably the conflict between privacy protection and public security preservation. Social security and public interest have long been an overarching value in Vietnam's tradition, culture and legislation as well. So the commitment to upholding the primacy of public security tends to pose serious threats to an individual's data privacy. Due to the fact that the language in the draft Decree grants broad investigatory powers to public security agencies, allowing them to collect and use personal data for the purpose of detecting and investigating criminal suspects, and the discretionary power for PDPC under the MPS to conduct the investigation and approve for sensitive data processing and overseas data transfer.

The current legal regime stipulates that exceptions on the collection and usage of data should be conducted if in line with relevant State's laws. However, by far, a lack of guidelines has denied clarity and created uncertainty, such provision is subject to the interpretation by the Courts in practice. The absence of meaningful legal control over public security agencies' collection of personal data could leave the Vietnamese government unlimited space in the development and usage of surveillance technologies. If Vietnam's future data privacy law fails to provide meaningful legal control over data collection e.g. for the purpose of criminal investigation,

such a law may facilitate government surveillance at worse.

In the context of low legislation in the new technology, carefulness in adopting the proper language may bring benefits for both the government and the enterprises. The current situation can allow the Government to continue to listen to business while partially achieving its objective of control whereas obscurity, certainty also enable companies to continue to develop their case in the face of light regulation while at the same time aligning at least in part with the government.

4. Legislation Development of Data Privacy Protection in Asia-pacific and Suitable Trend to Modify the Data Protection Law in Vietnam

4.1. Legislation Context in Data Privacy Protection in Asia-pacific

Under a report from United Nations Conference on Trade and Development (UNCTAD), as of January 2021, 128/194 nations had enacted legislation to provide data and privacy protection around the world. However, in Asia-pacific the data privacy landscape has just changed dramatically in the last decade, which indicates that the region's privacy regulations shall continue to evolve until 2021 and beyond. There is almost 34/60 countries (equal to 57%) give legislation for privacy protection while 6 countries is in the process of law drafting. Between 2010 and 2020, more than thirteen jurisdictions in Asia-pacific implemented new data privacy laws, while seven changed their existing laws (four of them amended the laws twice during this 10-year period) [21]. It is critical to highlight that there are no law-making unification as in the GDPR in EU or any binding treaties of data protection law in Asia - pacific or even sub-regional organisations in Asia for privacy protection. Therefore, privacy protection in Asian nations shall be studied in each national legislation and legal researches may focus on other elements surrounding democracy and the rule of law in each country, which might overshadow other issues.

In Asia, despite a two-decade history of data privacy, or data protection since 2000 as it is known elsewhere, major advances have occurred only in the last few years. The first international impact on the development of data privacy laws in Asia came from the OECD's Privacy Guidelines (1980) with the issuance of the Act on the Protection of Personal Information Held by Administrative Organs 1988 of Japan [22] and the Public Agency Data Protection Act 1995 of South Korea [23]. Being an OECD member, both Japan and South Korea followed a similar approach to several other OECD members outside Europe, particularly Australia (1988), Canada (1982), and (prior to the OECD Guidelines) the United States (1974). However, the Japanese Act only applies to paper-based data managed by administrative agencies and imposes fines for disclosures, whereas the Korean Act only applies to the public sector.

In 1995, Asia's first comprehensive data privacy law appeared when the colonial government of Hong Kong enacted the Personal Data (Privacy) Ordinance, which covered both the public and private sectors [6] But it is not until 2009 that Malaysia became the first ASEAN member to pass legislation governing the private sector in Malaysian Personal Data Protection Act [16]. Simultaneously, the Data Privacy Act of the Philippines and the Personal Data Protection Act of Singapore were adopted in 2012. Futher after this period, there are comprehensive amendments as well as regulations stronger data privacy laws in many Asia countries and colonies, include South Korea, Japan, Hongkong, Indonesia, Thailand, etc.

Under the strong impact of the legislative context in Asia-pacific, it is the right time for Vietnam to modify its legislation relating to data privacy protection to harmonise its domestic law with the general principles widely recognised in the region and the world.

4.2. A Need for Data Privacy Protection in Vietnam Facing the Strong Boost of the Internet and the Technical Development

Along with the Internet development in the 21st century, Vietnam is among the countries with the tremendous growth of Internet users in the Asia-pacific region. However, there are still some popular habits of violating other people's private lives and the infringement is brought to the next level through the internet.

Technical and social developments, including but not limited to social networks, big data (including data analytics), and cloud computing, may raise some new difficulties, but they generally intensify and encroach on pre-existing ones. Private life is being followed by prying, cameras, recorders, smartphones etc. Private information can be distributed not only by word-of-mouth, mailing, hand transmission but also can be shared uncontrollably over the Internet. The arbitrary use and sharing of other people's information have become a big problem, especially in some cases related to celebrities, political scandals or pandemic patient information etc.

On the internet, Vietnamese netizens usually regard privacy as normative behaviour, a socially prescribed manner of preventive action same as locking the door or keeping the bag carefully but not a right. Internet users appear to be more concerned with their money and reputation than their right to privacy [3]. The massive development of the internet and technology also leads to an asymmetry with the information technology infrastructure, making it difficult to detect and identify violations. The low awareness also makes people easily supply personal information for a platform, a website and allow others to freely access their information without any consideration.

Moreover, the right to privacy and right to access to information are closely related. Both of them are protected by international conventions and regulated in the constitutions of many countries, but they have one thing in common: the exemption of the right to access information is the protection of privacy. It is more controversial when some people claim that the public should be provided with adequate information and have the right to freely access information to promote innovation and growth, meanwhile some claim about the right to be forgotten/ right to erasure in the scope of the right to privacy.

The tug-of-war between the views on free-flow data and the views on protecting privacy is fierce. Especially in this age, since there is an electronic database, almost no one in society can completely keep any private facts about himself. In Vietnam, there is a lot of information and facts about individuals that are collected legally by state agencies and stored in databases controlled by the government. The privacy protection will just be meaningful if it is not an absolute right.

Therefore, it is necessary for Vietnam to have strict legal regulations to set a clear boundary so that the disclosure of private details must be very careful and selective and such laws can at least partially protect the right to privacy.

4.3. Upgrading Comprehensive Provisions and Principles Specific to the Collection, Storage and Use of Personal Information in Vietnam

Data protection requires a holistic approach to system design that incorporates a combination of legal, administrative, and technical safeguards [24]. Comprehensive data protection is composed of three categories: i) information or data privacy, ii) cybersecurity or data security, and iii) breach response. The privacy category includes the ownership, access, collection, and deletion of data. The security category includes the safekeeping, maintenance, and sharing of data. The response category includes notification, compensation, and penalties in case of a breach [25]. The legal framework should underpin safeguard individual data, privacy, and user rights.

In accordance with international standards on privacy and data protection, many countries adopted the laws which typically have broad

provisions and principles specific to the collection, storage and use of personal information. It seems that Vietnamese draft Decree is on the right track, but what the draft has done well is the legal recognition of the common principles, the draft lacks specific details and descriptions of the principle. Therefore, in the process of upgrading the current version of the Decree, Vietnam should focus on describing the legitimate interest of personal data processing, collection, and storage.

It has been a significant achievement of Vietnam since the mid-twentieth century to move from privacy protection to personal data protection. The country's efforts to build long-term development projects in personnel for cybersecurity were recognised, along with achievements in the creating of an ecosystem for safe "Made in Vietnam" products and cybersecurity [18].

Drawing on the aforementioned analysis on the existing data protection regime, the key reason is that legal challenges might be difficult to resolve in such a short time. An independent supervisory authority (the PDPC) is a fundamental element of most data protection laws worldwide and has not yet been established as a proper institution in Vietnam under the current version of the Decree, but we can believe the change of the approved Decree in the future. In the enactment of data privacy law, at least in the draft Decree, Vietnam must overcome the aforementioned obstacles.

References

[1] T. T. Hong, Hoàn thiện pháp luật về bảo vệ thông tin cá nhân ở Việt Nam hiện nay, 2018.

[2] World Bank, Individuals using the Internet (% of population)-Vietnam, 2020, https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=VN>, (accessed on: November 29th, 2021).

[3] Greenleaf, Graham, Asian Data Privacy Laws: Trade & human rights perspectives (first published 2014), Oxford, OX2 6DP.

[4] C. Schaefer, G. Greenleaf, Vietnam's Cyber-Security Law Strengthens Privacy,… A Bit, 141 Privacy Laws & Business International Report., 2016, pp. 26-27.

[5] Pernot-Leplay, Emmanuel, China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?, Penn State Journal of Law & International Affairs, 2020.

[6] Greenleaf, Graham, Data Privacy Laws in Asia Context and History, Asian Data Privacy Laws Trade and Human Rights Perspectives, Oxford University Press, 2014.

[7] Dallmayr, Fred, Asian Values and Global Human Rights, Philosophy East and West, 2002, pp. 173-89.

[8] L. Irwin, The GDPR: Legitimate Interest - What is it and When Does it Apply? (17th November 2020) https://www.itgovernance.eu/blog/en/the-gdpr-legitimate-interest-what-is-it-and-when-does-it-apply?> (accessed on: November 29th, 2021).

[9] W, Piemwichai, T. N. Tu, Vietnam's New Cybersecurity Law Will Have Major Impact on Online Service Providers', Tilleke & Gibbins, June 18th, 2018.

[10] Greenleaf, Graham, Vietnam: Data privacy in a Communist ASEAN state, 170 Privacy Laws & Business International Report, 2021, pp. 5-8.

[11] P. H. Duy, The Evolution Towards an ASEAN Human Rights Body, Asia-Pac J on Hum Rts & L, 2008, pp. 9.

[12] N. Shaun, Human Rights Norms and the Evolution of ASEAN: Moving Without Moving in a Changing Regional Environment, Contemporary Southeast Asia: A Journal of International and Strategic Affairs, Vol. 34, No. 3, 2012 pp. 88.

[13] C. Cui, An Interpretation of Confucian's Ethics of Cultivating One's Morality by Yi· DaXiang, Journal of Shiyan Technical Institute. 2009.

[14] Mower, Gordon B, Confucianism and Civic Virtue, Social philosophy today, 2013, pp. 75-87.

[15] P. N. Minh, L. Luong, N. L. Thanh, Completion of the Law in Order to Protect the Right to Privacy in the Current Social Environment of Vietnam, International Conference on Modern Educational Technology and Innovation and Entrepreneurship (ICMETIE 2020), Atlantis Press, 2020, pp. 171-179.

[16] B. H. Thiem, Civil Society and Governance in Vietnam's One Party System, Doctor of Philosophy at The University of Queensland, 2015, pp.81.

[17] J. Thomas, Cyber Warfare in Vietnam (4 October 2019), The Asian post,

https://theaseanpost.com/article/cyber-warfare-vietnam> (accessed on: November 29th, 2021).

[18] L. V. Ton, Russin & Vecchi, Cybersecurity in Vietnam has Anything Changed? https://www.lexology.com/library/detail.aspx?g=087ed1b5-aca4-4681-b27e-fb21572f6cda> (accessed on: November 29th, 2021).

[19] Southeast Asia Globe, Vietnam's Contact-Tracing App: Public Health Tool or Creeping Surveillance? (29th September 2020). https://southeastasiaglobe.com/bluezone-contact-tracing-app/ (accessed on: November 29th, 2021).

[20] Magdalena Kędzior, The Right to Data Protection and the COVID-19 Pandemic: the European Approach, ERA Forum Vol. 21, 2021, 533-543, https://doi.org/10.1007/s12027-020-00644-4.

[21] UNCTAD, Data Protection and Privacy Legislation Worldwide, 2021, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> (accessed on: November 29th, 2021).

[22] Srinivasan, Srinija, Privacy and Data Protection in Japan, Government Information Quarterly, 1992, pp. 121-133.

[23] Greenleaf, Graham, Whon-il Park, South Korea's Innovations in Data Privacy Principles: Asian Comparisons, Computer Law & Security Review, 2014, pp. 492-505.

[24] World Bank, Data Protection and Privacy Laws, https://id4d.worldbank.org/guide/data-protection-and-privacy-laws> (accessed on: November 29th, 2021).

[25] S. P. Mulligan, C. D. Linebaugh, W. C. Freeman, Data Protection and Privacy Law: An Introduction, Congressional Research Service (May 9th, 2019), https://fas.org/sgp/crs/misc/IF11207.pdf, (accessed on: November 29th, 2021).