sciendo
Vietnamese Journal of Legal Sciences, Vol. 11, No. 02, 2024, pp. 14-26 DOI: 10.2478/vjls-2024-0008

ADDRESSING FRAGMENTATION IN VIETNAM'S DATA PROTECTION LAWS: RECOMMENDATIONS FOR A UNIFIED LEGAL FRAMEWORK

NGUYEN HO BICH HANG
School of Law, University of Eastern Finland, Finland
Email: nhbhang@hcmulaw.edu.vn

Abstract

In the digital economy, general and personal data are vital for the success of individuals and businesses. Inadequate personal data protection infringes on an individual's fundamental rights and can jeopardize national security. Vietnam has enacted various measures but lacks a unified personal data protection law. This article examines Vietnam's personal data framework, compares it with regulations from the European Union's General Data Protection Regulation (GDPR), and references laws from Singapore, Thailand, and South Korea to highlight relevant legal matters.

Keywords: *data collection, data processing, data transfer, personal data, GDPR, Vietnam*
Received: 11 April 2024 / Revised: 12 June 2024 / Accepted: 31 July 2024

Data in general, personal data (PD) in particular, along with the current technological development, has become a type of "new oil" of the global sharing economy.[1] For PD's value, illegal PD transactions have occurred globally. The most recent data leak case is *AT&T*, which includes the personal information of 73 million customers. This incident happened in the United States at the end of March 2024 - customers' information, such as social security number, address, and more, out in the open.[2] The *Vastaamo* scandal in Finland in 2020 also exposed severe vulnerabilities in data protection. Established in 2008, Vastaamo operated as a subcontractor for Finland's public healthcare system. In 2020, a hacker seized the medical records of nearly 30,000 patients and extorted 450,000 euro in Bitcoin. Due to the lack of encryption, the hacker also blackmailed patients and threatened to publicize their sensitive information unless they paid him,[3] marking the worst cybersecurity breach in Finland's history.[4] Tens of thousands of victims suffered anxiety and stress, with long-lasting psychological effects.[5]

1 Radauer, A., Bader et al. (2022). Study on the legal protection of trade secrets in the context of the data economy (GRO/SME/20/F/206): Final report. European Commission.

2 Knutsson, K. (2024), 'AT&T data leak from 73 million customers; what you need to do next', CyberGuy Report, *Fox News*. Retrieved from: https://www.foxnews.com/tech/att-data-leak-what-you-need-to-do-next, [accessed 6 April 2024].

3 Ralston, W. (2021), 'They told their therapists everything. Hackers leaked it all', *Wired*. Retrieved from: https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/ [accessed 11 March 2024].

4 Traficom (2021), *Information Security in 2020 – Annual report of the National Cyber Security Centre Finland*, Traficom Publication, p. 3.

5 Cyber Peace Institute (2020), 'Vastaamo data breach - Attack on human security, dignity and equity'. Retrieved from: https://cyberpeaceinstitute.org/news/2020-10-28-vastaamo-data-breach-attack-on-human-security-dignity-and-equity/ [accessed 10 March 2024].

In Vietnam, similar incidents have occurred. In November 2023, Chợ Rẫy Hospital's website was hacked, resulting in malware being installed and control being seized.[6] Most recently, in March 2024, the online appointment scheduling website of Ho Chi Minh City Heart Institute was attacked, causing a system shutdown.[7] According to the "whitehat" top hacker Duong Ngoc Thai, if hospitals or healthcare centres do not secure health data, a hacker could infiltrate and alter any patient's medical records, endangering their health and lives.[8]

Overall, the potential for misuse of such data is significant, as it can be exploited for various malicious purposes. The uncertainty surrounding the long-term impacts on the affected individuals adds to the severity of the breach. The abovementioned examples raises critical questions about regulatory oversight in safeguarding personal data. In Vietnam, this reality calls for a robust legal framework to safeguard personal data. Yet, the framework for data protection in Vietnam is being fragmented.[9] While sectoral laws and decrees address aspects of data privacy and cybersecurity, they often lack the comprehensive scope needed to tackle modern data protection challenges. Additionally, there are still significant gaps and loopholes in personal data protection.

This article analyzes Vietnam's personal data protection framework, primarily comparing it with the European Union's General Data Protection Regulation (GDPR) and referencing laws from Singapore, Thailand, and South Korea to highlight key legal issues and suggest uniform laws to address fragmentation.

1. Vietnam's legal framework for protection of personal data, personal information

1.1. The 2006 Law on Information technology

The 2006 Law on Information technology (IT Law)[10] was enacted to regulate the application and development of information technology by agencies, organizations, and individuals in Vietnam. This is one of the first legal documents to regulate matters related to personal information in the online environment. Accordingly, the obligations of organizations and individuals who collect, process, and use personal information are quite strict

6 Dat, T. (2024), 'Bệnh viện có thể tê liệt vì hacker mã hoá dữ liệu tống tiền' [Hospitals can be crippled by hackers encrypting data for ransom]. Retrieved from: https://vietnamnet.vn/benh-vien-co-the-te-liet-vi-hacker-ma-hoa-du-lieu-tong-tien-2273268.html [accessed 3 June 2024].

7 Ibid.

8 Thai, D. N. (2023), 'Làm thế nào để giết một người và cả nền kinh tế', [How to kill a person and the whole economy]. Retrieved from: https://vnhacker.substack.com/p/lam-the-nao-e-giet-mot-nguoi-va-ca?utm_source=profile&utm_medium=reader2 [accessed 29 February 2024].

9 Walter, R., Novak, M. (2021), *Cyber security, artifical intelligence, data protection and the law,* Springer, p. 265.

10 The Law on Information technology was passed on 29 June 2006 and came into effect on 1 January 2007.

and progressive, specifically: (i) to inform individuals of the form, scope, place, and purpose of data use; (ii) use the information only for proper purposes and store it for a legally set period or as agreed; (iii) implement measures to prevent data loss, theft, disclosure, modification, or destruction.[11] Under the 2006 IT Law, individuals can request to inspect, correct, or cancel their data and seek compensation for damages caused by violations. Without consent or legal provision, personal information cannot be shared with third parties.[12]

The 2006 IT Law was influenced by the 1995 European Union's Data Protection Directive,[13] with Articles 21 and 22 closely resembling Articles 6-8 of the Directive. This influence has made the provisions of the 2006 IT Law related to personal information progressive. However, these regulations are impractical in reality, as evidenced by the ongoing illegal trading of consumer information or PD in Vietnam at various levels of complexity,[14] especially before the issuance of Decree No. 13/2023 on Personal Data Protection (Decree No. 13/2023).

It is worth noting that the 2006 IT Law does not use the term "personal data"; instead, the law refers to it as "personal information". These two terms are technically not the same.[15] Decree 52/2013 on E-commerce of the Government dated 16 May 2013 (Decree No. 52/2013),[16] which provides guidelines for the 2006 IT Law on e-commerce activities, contains the terms "personal data" and "consumer personal information".[17] This decree lacks a clear definition of PD, and its term "consumers' personal data" is nearly identical. Different terms in the 2006 IT Law and Decree No. 52/2013 show inconsistency and application challenges.

1.2. The 2015 Civil Code

In line with the 2013 Constitution which stipulates "everyone has the inviolable right to privacy, personal secrets, and family secrets…",[18] Article 38 of the 2015 Civil Code[19] recognizes individuals' right to privacy. Accordingly, individuals have certain types of information: (i) information about private

11 Article 21.1 of the 2006 IT Law.
12 Article 22 of the 2006 IT Law.
13 European Union Data Protection Directive enacted in October 1995.
14 Le, A. (2023), '5 vụ án mua bán dữ liệu cá nhân chấn động dư luận', [5 alarming cases of personal data trading that captured public attention]. Retrieved from: https://viettimes.vn/5-vu-an-mua-ban-du-lieu-ca-nhan-chan-dong-du-luan-post167800.html [accessed 30 March 2024].
15 Dammann, O. (2019), 'Data, Information, Evidence, and Knowledge: A Proposal for Health Informatics and Data Science', *Online Journal of Public Health Information*, Vol. 10, No. 3, 2019. Retrieved from: 10.5210/ojphi.v10i3.9631 [accessed 30 March 2024].
16 Decree No. 52/2013/ND-CP on E-commerce of the Government dated May 16, 2013 (Decree 52/2013).
17 Article 69.1 of the Decree No. 52/2013.
18 Article 21 of the 2013 Constitution Law.
19 The 2015 Civil Code was passed on 24 November 2015 and came into effect as from 1 January 2017.

life, (ii) personal secrets, and (iii) other private information, encompassing a broad scope that includes personal data. This approach aligns closely with the European Union's stance on privacy rights, in which PD is one of the components of privacy rights.[20] The rights to privacy and the protection of PD are regulated in the Charter of Fundamental Rights of the European Union,[21] forming the basis for the regulations on PD protection in Europe, such as the Data Protection Directive 1995, which is the precursor to the GDPR. With a similar approach, Vietnam has a strong foundation to enhance its data protection laws, better addressing modern challenges and ensuring the inviolable right to privacy for its citizens.

However, Article 38 of the 2015 Civil Code does not define what constitutes privacy or personal secrets but simply asserts: "The private life... is inviolable and protected by law", "the collection, storage, use, and publication of information related to private life, personal secrets must be consented to by the person, except in cases otherwise provided by law" and "the exposure, control, seizure… of electronic databases and other forms of private information exchange of others may only be conducted in cases prescribed by law". Both Article 38 of the 2015 Civil Code and the 2006 IT Law aim to protect PD, but while the 2006 IT Law provides specific guidelines for the tech sector, Article 38 of the 2015 Civil Code offers broader privacy protection. Therefore, the 2015 Civil Code does not regulate PD, which can be explained by the role of this code within the legal system. Given its role as the primary code for general individual issues, including PD in this code is unnecessary; PD-related matters can be addressed through specific sectoral laws.

1.3. The 2018 Cybersecurity Law

The 2018 Cybersecurity Law was enacted to address the challenges in the cyberspace environment, protect national security, and ensure social order and safety in cyberspace.[22] This law inherits the spirit of the 2006 IT Law and the 2015 Civil Code regarding personal information. The 2018 Cybersecurity Law uses the terms "private life" and "personal secrets" in Article 17. Like the 2015 Civil Code, it does not define these terms. Instead, this law includes provisions related to "data on personal information" and "user information,"[23] but it lacks specific terms or regulations about PD.

The 2018 Cybersecurity Law does not cover PD as it focuses on national security, cyberspace safety, and the responsibilities of relevant

20 Ong, R. (2023), 'Mandatory data breach notification: Its role in protecting personal data', *Journal of International and Comparative Law*, Vol. 10, No. 1, pp. 87–112.

21 Article 7 and 8 of the Charter of Fundamental Right of the European Union enacted on 2000.

22 Cybersecurity Law was passed on 12 June 2018 and came into effect on 1 January 2019 (2018 Cybersecurity Law).

23 Article 17.1(a) of the 2018 Cybersecurity Law.

agencies, organizations, and individuals.[24] It provides a legal foundation for protecting against cyberattacks and influences subsequent PD regulations. The law addresses seizing, buying, storing, or disclosing personal secrets affecting individuals' honour, dignity, and rights, as well as altering or damaging such information. Violators face disciplinary action, administrative penalties, or criminal prosecution and must compensate for damages.[25]

1.4. Decree No. 13/2023 on Personal data protection

Decree No. 13/2023 significantly advances Vietnam's legal framework for personal data protection by addressing definition gaps and enhancing safeguards against unauthorized access and misuse. The Decree defines PD as "information in the form of symbols, writing, numbers, images, sound, or similar on an electronic environment associated with a specific individual or helps identify a specific individual".[26] It can be inferred that almost all information related to an individual is considered PD. Under Decree No. 13/2023, PD is divided into (i) basic PD and (ii) sensitive PD.

- Basic PD includes name, date of birth, gender, place of birth, images, marital status, family relationships, and account numbers, identifying individuals. It is used in daily civil and commercial transactions, like signing contracts or engaging with state agencies. Basic PD is not covered by Article 38 of the 2015 Civil Code; violations are handled under Decree No. 13/2023.

- Sensitive PD includes political and religious views, health conditions, and private life details. Disclosure impacts individual rights, aligning with privacy protections in Article 38 of the 2015 Civil Code and Article 17 of the 2018 Cybersecurity Law. Strict confidentiality is required, especially in healthcare, according to the 2023 Law on Medical Examination and Treatment.[27]

The definition of PD in Decree No. 13/2023 closely aligns with that of the GDPR, particularly in regulating the form of PD: electronic/online environment.[28] This alignment is unsurprising, given that the GDPR serves as the primary reference for many countries in the Asia Pacific region when developing their own data protection regulations.[29]

Yet the Personal Data Protection Act (PDPA) of Singapore[30] covers data beyond electronic forms, while South Korea's Personal Information Protection

24 Article 1 of the 2018 Cybersecurity Law.
25 Article 9 of the 2018 Cybersecurity Law.
26 Decree No. 13/2023/ND-CP of the Government on Protection of Personal Data dated April 17, 2023 (Decree No. 13/2023).
27 Article 69.2 of the 2023 Law on Medical Examination and Treatment. This law was passed on 1 January 2023 and came into force as from 1 January 2024.
28 Article 4.1 of the GDPR.
29 Solove, D. J., Schwartz, P. M. (2024), *EU data protection and the GDPR*, Aspen, p. 89.
30 Singapore issued the Personal Data Protection Act (PDPA) in 2012, this law has been revised many times, the latest amendment was in 2021.

Act (PIPA) does not specify an electronic environment.[31] The protection of deceased individuals' personal data also varies: the GDPR[32] and Thailand's PDPA[33] do not address it, South Korea's PIPA is silent, and Singapore's PDPA protects data of individuals deceased for up to ten years,[34] while Decree No. 13/2023 addresses data processing for declared deceased individuals without a time limit.[35] This approach aligns with the GDPR and reflects adaptations seen in Singapore, Thailand, and South Korea, tailored to each country's context.

Under Decree No. 13/2023, processing PD requires the data subject's consent.[36] Data subjects must be informed about PD processing activities, and collection must be limited to the declared scope and purpose. PD cannot be traded unless provided by law.[37] Data subjects have rights to consent, access, withdraw consent, data erasure, restrict processing, data portability, and object to processing.[38] These rights are similar to those in the GDPR, although the GDPR is more comprehensive regarding the clarity, voluntariness, affirmation and content of consent.[39]

Violations of PD protection regulations can lead to disciplinary actions, administrative penalties, or criminal prosecution.[40] However, in Vietnam, decrees are subordinate to laws and provide detailed implementation guidelines. The role of Decree No. 13/2023 is limited by its hierarchical position, and the fragmented state of PD protection will persist if alignment issues among legal documents are not resolved.

1.5. The 2023 Law on Consumer Rights Protection

The 2023 Law on Consumer Rights Protection[41] includes provisions related to collecting and processing consumer information and data. Notably, the 2023 CP Law is closely associated with Decree No. 13/2023 concerning the regulations on consumer information. Consumer information comprises the personal information of consumers, information about the process of purchasing products, goods, services of consumers, and other information related to transactions between consumers and business organizations or individuals.[42] Thus, the scope of consumer information in the 2023 CP Law

31 Article 2.1 of the PIPA.
32 Recital 27 of the GDPR.
33 Personal Data Protection Act (PDPA) of Thailand was adopted in 2019 and came into force in 2022.
34 Article 4.4 of the PDPA of Singapore.
35 Conditions to declare a person is deceased are provided at Article 71 of the 2015 Civil Code.
36 Article 2.7, 2.8 of the Decree No. 13/2023.
37 Article 3 of the Decree No. 13/2023.
38 Article 9 of the Decree No. 13/2023.
39 Custers, B., Sears, A. M., Dechesne, F., Georgieva, I., Tani, T., Hof, S. V. D. (2019), *EU personal data protection in policy and practice*, Springer, p. 2.
40 Article 4 of the Decree No. 13/2023.
41 The Law on Protection of Consumer Rights was passed on 20 June 2023, and came into effect on 1 July 2024 (2023 CP Law).
42 Article 3.3 of the 2023 CP Law.

is similar to the "user information" regulations in the 2018 Cybersecurity Law. Consumer information in the 2023 CP Law encompasses both basic PD and sensitive PD as regulated in Decree No. 13/2023. Products or services are sensitive, leading consumers to prefer to keep them private. Therefore, without explicitly delineating in the 2023 CP Law, handling sensitive PD of consumers could have loopholes.

The 2023 CP Law introduces the concept of protecting vulnerable consumers,[43] recognizing those more susceptible to adverse impacts in legal transactions. Vulnerable consumers include the elderly, disabled people, children, ethnic minorities, pregnant women or women nursing children under 36 months, people with serious illnesses, and members of poor households. These consumers face disadvantages in accessing information, health, assets, and dispute resolution. Nevertheless, this law does not address the collection and use of information from vulnerable consumers. For instance, ethnic minorities in remote areas or those in difficult living conditions who have a low legal awareness are at higher risk of unlawful information collection. If the 2023 CP Law classifies consumers into two groups, it should regulate the protection methods for each group accordingly. This oversight may be addressed in future regulations to overcome the gap between Decree No. 13/2023 and the 2023 CP Law.

2. Measures for personal data violation under Vietnam's regulations

With 73% of Vietnam's population accessing the Internet,[44] unauthorized PD collections are common.[45] PD is widely traded, and weak sanctions make prevention ineffective.[46] Protecting PD thus becomes critical, primarily when Vietnam aims to develop e-government, digital economy, digital society, and digital citizens.[47] Rapid cyber infrastructure growth has outpaced the legal framework for PD, making current sanctions ineffective due to a lack of a specific law. Additionally, fragmented regulations complicate enforcement.

2.1. Administrative measures

Administrative fines under the GDPR consider factors like the

43 Article 8 of the 2023 CP Law.

44 VOV (2023), 'Để quyền lợi người tiêu dùng không bị xâm phạm trong bối cảnh hiện nay' [To ensure consumer rights are not violated upon in the current context]. Retrieved from: https://vov.vn/kinh-te/de-quyen-loi-nguoi-tieu-dung-khong-bi-xam-pham-trong-boi-canh-hien-nay-post1060990.vov [accessed 11 March 2024].

45 Hien, N. (2023), 'Bộ Công an: Nhiều dữ liệu cá nhân, nội bộ bị thu thập, mua bán trái phép' [Ministry of Public Security: Many personal and internal data are collected and sold illegally]. Retrieved from: https://vov.vn/phap-luat/bo-cong-an-nhieu-du-lieu-ca-nhan-noi-bo-bi-thu-thap-mua-ban-trai-phep-post1025015.vov [accessed 29 December 2023].

46 Government (2023), 'Nghị định số 13/2023/NĐ-CP: Bảo vệ quyền dữ liệu cá nhân; ngăn chặn các hành vi xâm phạm dữ liệu cá nhân' [Decree No. 13/2023/NĐ-CP: Protection personal data; preventing personal data breaches]. Retrieved from: https://xaydungchinhsach.chinhphu.vn/nghi-dinh-13-2023-nd-cp.html [accessed 11 March 2024].

47 Hien, N. (2023), *supra* note 45.

infringement's nature, gravity, duration, affected data subjects, damage level, intent, mitigation efforts, and responsibility, guiding case-by-case decisions.[48] The maximum administrative fines under the GDPR in case of multiple infringements are up to 20 million EUR or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[49] The fines at EU levels that are set by GDPR have considerably increased in comparison to the EU Member States.[50] This level of fine is reasonable in the current situation where PD can be processed, transferred, and traded globally easily. Once a PD breach occurs, it would impact thousands or millions of individuals.

Decree No. 15/2020 applies to violations of regulations on storing, leasing, transmitting, providing, accessing, collecting, processing, exchanging, and using personal information illegally.[51] Administrative penalties under this decree are implemented for violations related to collecting and using personal information,[52] updating, modifying, and deleting personal information,[53] and violating regulations on ensuring the safety of personal information online.[54] The fines in this decree are low, ranging from VND 10 million (USD 400) to VND 70 million (USD 2800), insufficient to deter illegal PD transactions. Infringers must remove illegally collected data. Decree No. 15/2020 specifies "private information of telecommunication service users", not PD, causing potential regulatory gaps and uneven enforcement.

2.2. Criminal measures

The GDPR does not directly stipulate criminal measures but leaves this to Member States, which can impose criminal penalties for infringements.[55] These penalties may include depriving profits from GDPR violations. Article 84 mandates effective, proportionate, and dissuasive penalties, tailored to each nation's conditions. In Vietnam, Article 288 of the 2015 Penal Code[56] regulates the offence of illegally providing or using information on computer or telecommunications networks. This article specifies the acts of trading, exchanging, giving, changing, or publishing lawfully private information of an individual on the computer or telecommunications networks without the

48 Article 83 of the GDPR.
49 Article 83.6 of the GDPR.
50 Voigt, P., Bussche, A. V. D. (2017), *The EU General Data Protection Regulation (GDPR): A practice guide*, Springer, p. 209.
51 Decree No. 15/2020/ND-CP dated 3 February 2020 on penalties for administrative violations in postal services, telecommunications, radio frequencies, information technology and electronic transactions (Decree No. 15/2020).
52 Article 84 of the Decree No. 15/2020.
53 Article 85 of the Decree No. 15/2020.
54 Article 86 of the Decree No. 15/2020.
55 Recital 149 of the GDPR.
56 The Penal Code was passed on 27 November 2015 (the 2015 Penal Code).

permission of the information's owner.[57] Depending on the nature and the seriousness of the violation, Article 288 provides monetary fines, community sentences, imprisonment, or prohibition from holding certain positions or doing certain jobs.

Article 288 of the 2015 Penal Code specifies two types of damages: (i) material and (ii) non-material. Material damages require a threshold of VND 50 million (approx. USD 2000) for illegal profit gains and VND 100 million (approx. USD 4000) for causing material damage. Non-material damage includes privacy infringements leading to suicide, or impacts on social security, order, safety, or Vietnam's diplomatic relations. The 2015 Penal Code's vague language complicates identifying non-material consequences,[58] emphasizing material damages while neglecting non-material harms like psychological distress and loss of trust from large-scale PD breaches. Furthermore, Article 288 of the 2015 Penal Code refers to "an individual's legal private information", rather than PD, which makes it more challenging to enforce criminal sanctions for breaches involving personal data. This distinction can hinder the pursuit of justice and, due to the legality principle "*nullum crimen sine lege*" (no crime without law), further complicates the application of criminal sanctions.[59] Thus, another challenge for the Code includes standardizing legal terms and addressing non-material damages to better protect citizenship rights and prevent crimes.

2.3. Civil measures

Under Decree No. 13/2023, data subjects can claim damage for PD protection violations.[60] The right to claim damage is a civil measure recognized in the 2015 Civil Code, which states, "anyone who infringes upon the honour, dignity, prestige of another person causing damage must compensate".[61] Current regulations allow individuals to claim compensation for both material and non-material damage. The code requires full and prompt compensation for actual damage, with the amount to be agreed upon by the parties unless otherwise provided by law.[62] For mental suffering, under Article 592, if the parties are not able to agree, the maximum sum shall not exceed a ten-month base salary prescribed by the State (approximately 18 million VND, equivalent

57 Article 288.1(b) of the 2015 Penal Code.

58 Tung, T. Q. (2021), 'Tội phạm đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông - Những khó khăn, vướng mắc trong phát hiện, điều tra, xử lý và giải pháp khắc phục' [Illegal provide or use of information on computer networks or telecomunications networks - Difficulties and obstacles in detection, investigation, processing, and solutions to overcome], *Journal of Procuracy Science*, Vol. 47, Special No. 1, p. 26.

59 Article 2 of the 2015 Penal Code.

60 Article 10.9 of the Decree No. 13/2023.

61 Article 584 of the 2015 Civil Code.

62 Article 585.1 of the 2015 Civil Code.

to 720 USD).[63]

However, Article 592 of this Code is not specifically designed to protect PD. Considering that PD breaches can impact thousands of individuals, a critical question arises: can each victim feasibly claim compensation? This issue warrants serious consideration, as the effectiveness of mental suffering compensation as a deterrent is undermined. The courts in certain countries, including the United States, have dismissed claims for mental damages, stating that "theft of personal information alone does not produce recognizable losses". Many courts only accept cases with actual damages due to inadequate PD protection.[64] Some courts required an "injury in fact".[65] Therefore, effective enforcement in Vietnam necessitates legal measures that correspond to the nature of infringement acts and consider the fragile nature of PD.

3. General assessment and recommendations

Overall, fragmentation in PD regulations can lead to confusion and inefficiency in law enforcement, and this is caused by a sectoral approach. When sectoral laws regulate aspects of personal information, they ensure that specific content related to individuals is governed in detail. Conversely, the "siloed" approach within different legal sectors regarding the same content can create overlaps and loopholes. This situation is evident in the current regulations on personal information, privacy secrets, individual secrets, consumer information, and personal data, which are not fully harmonized in the 2006 IT Law, the 2015 Civil Code, the 2015 Penal Code, the 2018 Cybersecurity Law, the 2023 CP Law, and other subordinate legal documents, especially Decree No. 13/2023. The lack of unified terminology and comprehensive terms creates challenges in legal application and enforcement. Furthermore, current sanctions are ineffective in preventing violations of personal, consumer, and PD information, making such breaches common. Because of the borderlessness of the digital environment, information and PD are illegally traded internationally. Decree No. 13/2023 lacks clear sanctions for adequate PD protection.

3.1. The essential enactment of the Law on Personal data protection

Based on the aforementioned analysis, it is evident that Decree No. 13/2023, as a bylaw, addresses urgent PD protection issues in Vietnam but

63 Resolution of the National Assembly on the 2023 State's Budget Estimate dated 11 November 2022.

64 Solove, D. J. and Keats, C. D. (2017), 'Risk and anxiety: A theory of data breach harms', *GWU Law School Public Law Research Paper*, Vol. 2, p. 3.

65 Cheong, B. C. & Mohamed, K. A., 'Personal data beach claims for emotional distress and loss of control in the Singapore Court of Appeal', p. 3. Retrieved from: https://ssrn.com/abstract=4700172 [accessed 11 March 2024].

lacks comprehensive coverage. PD's critical role necessitates an integrated legal approach, highlighting the need for a dedicated Law on Personal Data Protection (Law on PDP) to resolve fragmentation and ensure effective PD protection.[66] Asia-Pacific countries, like Singapore, Thailand, and South Korea, initially regulated PD through sectoral laws or *ad hoc* approaches.[67] Later, they adopted an umbrella approach by enacting comprehensive PD protection laws. For example, Singapore's PDPA covers sector-specific regulations, including banking insurance. South Korea's PIPA was enacted as an attempt to consolidate and create an umbrella privacy law.[68] In Thailand, PD-related matters were governed by sectorial laws such as the Constitution, Banking and Finance, Telecommunication, and Child Protection and Electronic Transactions Act,[69] before the issuance of the comprehensive PDPA in 2019. Thus, these countries are regulating aspects of data protection closer to the European model[70] or influenced by GDPR.[71] As globalization and digital transformation accelerate, an umbrella Law on PDP in Vietnam would enhance consistency and address fragmented regulations. It should incorporate sector-specific regulations for banking, insurance, and telecommunications, while standardizing the terminology, scope, and duration of personal data processing.

3.2. Proposals for more robust enforcement mechanisms

Without strong enforcement, even the most comprehensive legal framework can fail to protect personal data adequately. Vietnam must develop stringent enforcement strategies, including administrative, criminal, and civil measures, along with punitive damages, to effectively safeguard personal data and uphold privacy rights.

For civil measures, under the Vietnamese legal framework, data subjects can claim damages for PD leakage according to the 2015 Civil Code. This code mandates compensation for harm to life, health, honour, dignity, reputation, property, or other legal rights.[72] Depending on the case, data subjects can seek compensation for material or mental damages. In the EU, Article 82.1 of the GDPR grants the right to compensation for material or non-material damage resulting from an infringement, with the CJEU

66 Walter, R., Novak, M. (2021), *supra* note 9, p. 285.

67 Chesterman, S. (ed) (2014), *Data protection law in Singapore: Privacy and sovereignty in an interconnected world*, Academy Publishing, p. 10.

68 Westby, J. R. (ed) (2004), *International guide to privacy*, Section of Science & Technology Law, p. 124.

69 Walters, R., Trakman, L., Zeller, B., (2019), *Data protection law – A comparative analysis of Asia-Pacific and European Approaches*, Springer, p. 218.

70 Chesterman, S. (ed) (2014), *supra* note 67.

71 United Nations Conference on Trade and Development (2022), *Voluntary peer review of consumer protection law and policy of Thailand*, United Nations, p. 24.

72 Article 584.1 of the 2015 Civil Code.

clarifying that this establishes a fault-based liability regime, emphasizing that compensation must fully address the actual damage suffered.[73] Non-material damages do not need a "*de minimis* threshold" to be compensable,[74] as this would conflict with the GDPR's aim of high PD protection. Individuals must simply demonstrate that the negative consequences constitute non-material damage under Article 82 of the GDPR. Learning from the EU's approach, for PD violations affecting an individual's honor and reputation, mental damages should be claimable if the causal link to the anxiety and stress endured by themselves and their families is proven.[75] Adopting provisions for non-material damage would strengthen Vietnam's legal framework for PD protection, enhancing mechanisms for data subjects and aligning with international standards.

Regarding punitive damage measure, the 2015 Civil Code does not apply punitive damage, but to deter illegal PD activities, Vietnam should consider them. South Korea's PIPA allows for punitive damages up to five times the actual damages.[76] Similarly, Thailand's PDPA is up to twice.[77] The Law on PDP could adopt a range of 2 to 5 times the actual damage, depending on the PD breach's severity. This would serve as a strong deterrent, emphasize the importance of PD protection, and penalize violators beyond mere restitution, reflecting the need to prevent such breaches. ●

References

**** Cases***

[1] *Case C-667/21 ZQ v. Medizinischer Dienst*

[2] *Case C-456/22 VX, AT v. Gemeinde Ummendorf*

**** Books and Articles***

[3] Cheong, B. C. & Mohamed, K. A., 'Personal data beach claims for emotional distress and loss of control in the Singapore Court of Appeal'. Retrieved from: https://ssrn.com/abstract=4700172 [accessed 11 March 2024]

[4] Chesterman, S. (ed) (2014), *Data protection law in Singapore: Privacy and sovereignty in an interconnected world*, Academy Publishing

[5] Custers, B., Sears, A. M., Dechesne, F., Georgieva, I., Tani, T., Hof, S. V. D. (2019), *EU personal data protection in policy and practice*, Springer

[6] Cyber Peace Institute (2020), 'Vastaamo data breach - Attack on human security, dignity and equity'. Retrieved from: https://cyberpeaceinstitute.org/news/2020-10-28-vastaamo-data-breach-attack-on-human-security-dignity-and-equity/ [accessed 10 March 2024]

73 *Case C-667/21 ZQ v. Medizinischer Dienst.*

74 *Case C-456/22 VX, AT v. Gemeinde Ummendorf.*

75 Article 2.1 of the Resolution 02/2022/NQ-HĐTP on guidelines for application of some provisions of the Civil Code on tort liability of the Council of Judges of Supreme People's court on 6 September 2022.

76 Article 39.3 of the PDPA of South Korea.

77 Article 78 of the Thailand's PIPA.

[7] Dammann, O. (2019), 'Data, information, evidence, and knowledge: A proposal for health informatics and data science', *Online Journal of Public Health Information*, Vol. 10, No. 3, 2019. Retrieved from: 10.5210/ojphi.v10i3.9631 [accessed 30 March 2024]

[8] Dat, T. (2024), 'Bệnh viện có thể tê liệt vì hacker mã hoá dữ liệu tống tiền' [Hospitals can be crippled by hackers encrypting data for ransom]. Retrieved from: https://vietnamnet.vn/benh-vien-co-the-te-liet-vi-hacker-ma-hoa-du-lieu-tong-tien-2273268.html [accessed 3 June 2024]

[9] Knutsson, K. (2024), 'AT&T data leak from 73 million customers: What you need to do next', CyberGuy Report, *Fox News*. Retrieved from: https://www.foxnews.com/tech/att-data-leak-what-you-need-to-do-next, [accessed 6 April 2024]

[10] Ong, R. (2023), 'Mandatory data breach notification: Its role in protecting personal data', *Journal of International and Comparative Law*, Vol. 10, No. 1. Retrieved from: https://ssrn.com/abstract=4480675 [accessed 11 March 2024]

[11] Ralston, W. (2021), 'They told their therapists everything. Hackers leaked it all', *Wired*. Retrieved from: https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/ [accessed 11 March 2024]

[12] Solove, D. J., Schwartz, P. M. (2024), *EU Data Protection and the GDPR*, Aspen

[13] Solove, D. J. and Keats, C. D. (2017), 'Risk and anxiety: A theory of data breach harms', *GWU Law School Public Law Research Paper*, Vol. 2

[14] Radauer, A., Bader et al. (2022). Study on the legal protection of trade secrets in the context of the data economy (GRO/SME/20/F/206): Final report. European Commission

[15] Thai, D. N. (2023), 'Làm thế nào để giết một người và cả nền kinh tế', [How to kill a person and the whole economy]. Retrieved from: https://vnhacker.substack.com/p/lam-the-nao-e-giet-mot-nguoi-va-ca?utm_source=profile&utm_medium=reader2 [accessed 29 February 2024]

[16] Traficom (2021), *Information Security in 2020 – Annual report of the National Cyber Security Centre Finland*, Traficom Publication

[17] United Nations Conference on Trade and Development (2022), *Voluntary peer review of consumer protection law and policy of Thailand*, United Nations

[18] Voigt, P., Bussche, A. V. D. (2017), *The EU General Data Protection Regulation (GDPR): A practice guide*, Springer

[19] Walter, R., Novak, M. (2021), *Cyber security, artifical intelligence, data protection and the law,* Springer

[20] Walters, R., Trakman, L., Zeller, B., (2019), *Data protection law – A comparative analysis of Asia-Pacific and European Approaches*, Springer

[21] Westby, J. R. (ed) (2004), *International guide to privacy*, Section of Science & Technology Law

Author Contribution

The author solely contributed to the study conception and design. The author read and approved the final manuscript.

Declarations

Conflict of Interest: The author declares no competing interests.

Disclaimer: All claims expressed in this article are solely those of the author and do not necessarily represent those of the author's affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article or claim that may be made by its manufacturer is not guaranteed or endorsed by the publisher.