

Enhancing Vietnamese criminal law on personal data protection in cyberspace to foster cooperation with the European Union

Nguyen Thi Anh Hong
Tran Thanh Thao

Faculty of Criminal Law
Ho Chi Minh City University of Law
2 Nguyen Tat Thanh, Ward 13, District 4
Ho Chi Minh City, Vietnam
ntahong@hcmulaw.edu.vn
ttthaohs@hcmulaw.edu.vn

Abstract: Protecting personal data in cyberspace is an issue of significant concern to many countries around the world, including Vietnam. The invasion of personal data in cyberspace is currently common in Vietnam; however, these dangerous acts have not been dealt with effectively because of gaps in Vietnamese law regarding personal data in general and Vietnamese criminal law concerning these crimes in particular. By applying analytical-logical and comparative methods, this article aims to refine the provisions of Vietnamese criminal law on personal data protection in cyberspace. Starting by analyzing the provisions related to acts of personal data violation in cyberspace according to Vietnamese law and the shortcomings in their practical application, this article looks at European Union laws, specifically the *General Data Protection Regulation* and the *Budapest Convention on Cybercrime*. It then proposes some recommendations for improving Vietnamese criminal law regarding personal data violations in cyberspace to ensure compatibility between Vietnamese law and EU law.

Keywords: *European Union, Budapest Convention, cybercrime, cyberspace, General Data Protection Regulation, personal data protection, Vietnamese criminal law*

1. Introduction

Personal data refers to important information associated with each individual and personal data protection is closely related to human rights and information security. Due to the fact that protecting personal data not only safeguards individuals' privacy regarding their information but also ensures the development and safety of society, it is necessary to establish appropriate protective measures. Personal data violations in cybercrime in Vietnam have recently been more serious, however, the law enforcement is still ineffective (The Ministry of Public Security, 2024).

Personal data protection stands as one of the most important areas within the comprehensive cooperation framework between Vietnam and the European Union (EU). Notably, the *Framework Agreement on Comprehensive Partnership and Cooperation* (2012) between the Socialist Republic of Vietnam, the EU and its member states, signed on June 27, 2012, underscores this issue. Accordingly, the parties agree to cooperate to improve the level of personal data protection to the highest international standards as appropriate, such as those contained in international instruments, in so far as they apply to parties (*The Framework Agreement*, 2012).

The EU has extensive legal and practical experience in protecting personal data. Since 1981, the Council of Europe has issued the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (de Terwangne, 2021; Zolkin, Chochia and Hoffmann, 2023; Tropp, Hoffmann and Chochia, 2022). However, the EU recognized the demand to amend provisions on personal data protection due to advancements in science and technology and the new digital economy. Therefore, on April 14, 2016, the European Parliament adopted the *General Data Protection Regulation (GDPR)*, which aims to protect personal data and the privacy of individuals within the EU. In addition, regarding the field of criminal law, the Council of Europe also issued the *Convention on Cybercrime* in 2001 (hereafter, the *Budapest Convention*), which includes provisions directly related to offences against personal data protection in cyberspace. Although Vietnam is not a member of the *GDPR* or the *Budapest Convention*, provisions in these two legal documents are important legal standards that should be considered for reference in the process of refining Vietnamese criminal law concerning offences against personal data protection in cyberspace.

By applying analytical-logical and comparative methods, this article aims to refine the provisions of Vietnamese criminal law on personal

data protection in cyberspace by addressing two key research questions: (1) What are the shortcomings of Vietnamese criminal law in terms of personal data protection in cyberspace? and (2) What recommendations should be proposed to address these shortcomings?

2. Current legal regulations of Vietnam on personal data infringement in cyberspace and practical application in Vietnam

2.1 Regulations of Vietnam

Personal data, under ‘Decree No. 13/2023/ND-CP on the Protection of Personal Data’, refers to information in the form of symbols, letters, numbers, images, sounds or similar formats in electronic environments that are associated with a specific individual or help to identify a specific individual (‘Decree No. 13/2023/ND-CP’, Article 2(1)). According to this Decree, the right to protect personal data is recognized in Vietnamese law, and it stipulates prohibited acts related to personal data (‘Decree No. 13/2023/ND-CP’, Article 8). Accordingly, these prohibited acts are acts that may infringe upon the rights and interests of data subjects or use personal data as a means to commit violations against national security, public safety or public order. However, the enforcement of these provisions is ineffective because there are 69 legal documents directly related to personal data protection in Vietnam (The Ministry of Public Security, 2024), rather than a single unified legal document. For instance, to determine whether personal data processing violates legal regulations, competent authorities must refer to various legal documents, such as ‘Decree No. 53/2022 guiding the Law on Cyber Security’, ‘Circular No. 06/2023/TT-BNV on the management of civil servant data’, in addition to ‘Decree No. 13/2023/ND-CP on the Protection of Personal Data’. These legal documents are issued by different competent authorities and are sometimes inconsistent, which affects their implementation.

Not only are there many relevant legal documents, but most current legal documents on personal data protection in Vietnam are sub-law documents (such as decrees, circulars and decisions) and do not fully reflect the importance of personal data protection. Many provisions are vague and general, resulting in a lack of specific guidance for application in each specific case. Basically, the general legal framework governing the protection of personal data under Vietnamese law is mainly concentrated in ‘Decree No. 13/2023’, and this Decree’s provisions do not meet the necessary legal requirements to protect personal data.

Since the general legal framework on personal data protection is considered the foundation for specifying violations of personal data protection regulations, such as regulations on administrative sanctions or criminal offenses related to personal data, the development and promulgation of the *Law on Personal Data Protection* is necessary to establish a legal framework to specify and improve regulations in specific areas, ensuring a comprehensive approach to addressing personal data violations.

In addition to 'Decree No. 13/2023', the *Penal Code (Vietnam) 2017* (hereafter referred to as the *PCV*) also has a number of provisions related to personal data protection. Accordingly, individuals may be criminally liable for any of the following acts, depending on the type of act they commit, and may be criminally prosecuted for one of the following offences:

- 1) Unlawfully providing or using information on computer networks or telecommunication networks (*PCV*, Article 288). The objective element of this offense involves the intentional act of uploading information onto computer networks or telecommunication networks in violation of legal provisions (not falling under the provisions of Articles 117, 155, 156 and 326 of the *Penal Code*) (*PCV*, Article 288(1)). People who trade, exchange, gift, change, alter or disclose legal private information about organizations, entities or individuals on computer networks or phone networks without the information owner's permission are also guilty of this crime (*PCV*, Article 288(1)). This offense is particularly prevalent in personal data, especially the unauthorized trading or exchange of personal data without the consent of the data owner.
- 2) Unauthorized access to computer networks, telecommunication networks, or electronic devices of others (*PCV*, Article 289). Bypassing warnings, access codes or firewalls on purpose; using someone else's administrative rights; or using other methods to illegally access computer networks, telecommunication networks or electronic devices of others to take control, mess with the functionality of electronic devices, steal, change, destroy, forge data or use services without permission is considered this offense (*PCV*, Article 289(1)).
- 3) Using computer networks, telecommunication networks and electronic means to commit acts of property appropriation (*PCV*, Article 290). The objective part of this offense involves personal data and it happens when the offender utilizes information regarding the accounts or bank cards of organizations, entities or individuals to misappropriate the property of account holders or cardholders, or to pay for goods or services. It also includes the use of another person's data to create, store, trade, use

- or circulate counterfeit bank cards to misappropriate the property of account holders or cardholders, or for paying for goods or services (*PCV*, Article 290(1)).
- 4) Illegally collecting, storing, exchanging, trading or disclosing information about bank accounts (*PCV*, Article 291). This offense is constituted when an individual engages in the act of illegally collecting, storing, exchanging, trading, or disclosing information about another person’s bank accounts, which constitutes personal data. The act becomes a criminal offense when it involves 20 or more bank accounts or generates an illicit profit of VND 20 million or more (*PCV*, Article 291(1)).

2.2 Practical application in Vietnam

According to reports of the Supreme People’s Court of Vietnam from 2018 to 2024, the prosecution of crimes related to personal data protection in cyberspace is described in Table 1.

Table 1: Statistics on prosecution of crimes related to the protection of personal data in cyberspace (Source: Supreme People’s Court (Vietnam), 2024.)

<i>Penal Code article</i>	Cases	Defendants
Article 288	22	63
Article 289	38	74
Article 290	421	733
Article 291	71	168

According to this Table, among crimes related to the protection of personal data in cyberspace, the crime of using computer networks, telecommunications networks and electronic means to commit acts of property appropriation accounts for the majority. This is largely driven by the impact of the Industrial Revolution 4.0, where technology continues to evolve, leaving many users vulnerable due to insufficient knowledge about network security and susceptibility to sophisticated scams. In addition, the proliferation of various types of social networks creates an ideal environment for criminals to approach users to steal personal information (Anh, 2024). According to the statistics of the Ministry of Public Security, the amount of illegally collected and traded personal data has reached thousands of GB, including many internal and sensitive personal data (The Ministry of Public Security, 2024). In 2022, a serious personal data breach occurred

in Vietnam, involving the sale and public disclosure of approximately 6.2 million personal data in cyberspace (Van, 2022). The violators illegally profited nearly 3 billion VND and were consequently prosecuted under Article 288 of the *PCV* (Van, 2022).

However, the prosecution of criminal offenses related to the protection of personal data in cyberspace remains limited and does not fully reflect the actual extent of legal violations. The provisions of the *PCV* are ineffective as they fail to allow prosecution in certain cases. For instance, according to Article 288(1) of the *PCV*, criminal liability can only be imposed if the violator is proven to have unlawfully profited at least 50 million VND or caused damage to the victims of at least 100 million VND. Nevertheless, in a 2023 case in Thai Nguyen province, the violator was not prosecuted for illegally collecting and disclosing the personal data of over 10,000 individuals because the consequences could not be proven (Ministry of Information and Communications, 2022).

Additionally, technical legislative limitations regarding the crime of personal data breach in cyberspace under the *PCV* negatively impact prosecution efforts. Currently, Articles 288, 289, 290, and 291 of the *PCV* list specific violations as crimes. For example, Article 289(1) states that breaking these rules means “bypassing warnings, access codes, firewalls...”. It can be seen that, due to the rapid advancement of science and technology, the approach of listing the objective elements of crimes involving violations of personal data in cyberspace is ineffective and outdated compared to the actual methods of committing them. Also, the rules about the objective parts of crimes involving the theft of personal information in cyberspace are similar to those for other crimes. For example, some actions outlined in Article 289 are redundant with those listed in Articles 286 and 287. Therefore, it is necessary to amend the legislative technique regarding crimes involving personal data violations in cyberspace in the *PCV*.

It is worth noting the fact that Vietnamese criminal law has not yet recognized legal entities as subjects of crimes involving personal data infringement. As a result, individuals committing these offenses can only face criminal liability, while legal entities can only face administrative or civil liability. However, the fines under Vietnamese law are not sufficiently deterrent. Pursuant to Article 101 and Article 102 of ‘Decree No. 15/2000/ND-CP’, the maximum fine is only VND 70 million (approximately €30,000), while the damage caused is often significantly greater. Meanwhile, demanding compensation from a legal entity under civil law is highly challenging, as the claimant is

required to prove that the damage resulted from the legal entity's violation of personal data protection. The failure to hold legal entities criminally liable for these offenses negatively impacts efforts to prevent crimes involving personal data violations in cyberspace in Vietnam. In fact, legal entities predominantly commit personal data violations in cyberspace in Vietnam, including illegal collection, trade, and disclosure (Nguyen and Tran, 2024). In 2023, the Ministry of Public Security investigated 16 cases related to the disclosure, sale and loss of internal data in cyberspace by legal entities (Anh, 2024). However, under the current provisions of Vietnamese criminal law, only individuals who commit offenses stipulated in Articles 288, 289, 290 and 291 of the *PCV* can be subject to criminal liability. Consequently, legal entities cannot be held criminally liable in these cases.

Particularly in Vietnam, crimes related to personal data infringement often target children as victims. Accordingly, the 2022 report *Disrupting harm in Viet Nam: evidence on online child sexual exploitation and abuse* by ECPAT, INTERPOL and UNICEF (2022a) brings up the issue of Vietnamese children being subjected to unauthorized sharing of pornographic images in cyberspace. This situation has severely impacted the normal development of children. The unauthorized sharing of pornographic images of child victims in cyberspace, which can be widely disseminated and repeatedly viewed worldwide, causes victims to feel ashamed and constantly fear being recognized or discovered by acquaintances. However, the handling of violations related to the possession and dissemination of child sexual abuse materials has not been effectively implemented, significantly affecting the rights and interests of children. This is due to the fact that Vietnamese law has not clearly defined the crimes associated with the violation of sensitive personal information about children, such as having and illegally sharing pictures or videos of child sexual abuse online. Additionally, according to the report entitled *Legislation addressing online child sexual exploitation and abuse*, Vietnam has not yet defined child sexual abuse materials according to international standards, nor has it criminalized the act of unlawfully possessing such materials (ECPAT, INTERPOL and UNICEF, 2022b). This omission significantly impacts child victims, as child sexual abuse materials often contain sensitive information linked to the victim's identity. In fact, there was a case involving the distribution of child pornography, but the perpetrator could not be prosecuted for this act. The offender took advantage of the victim's acquaintance and took nude photographs of her when she was only 12 years old. He raped the victim and distributed the pornographic images online. However, he was only held criminally responsible for the

crime of child rape. Regarding the possession and distribution of child pornography, he was not held criminally responsible (The People's Court of Phu My, 2022). The failure to define child sexual abuse materials in accordance with international standards and to regulate the unlawful possession and dissemination of such materials in cyberspace does not create a legal basis for protecting children's personal data in cyberspace. Furthermore, the provisions regarding the protection of children's personal data in cyberspace under Vietnamese law are deemed incompatible with international standards.

3. Provisions on the protection of personal data and related offences under the *GDPR* and the *Budapest Convention*

3.1 The *General Data Protection Regulation*

The *General Data Protection Regulation (GDPR)* 2016/679 is a regulation in EU law concerning the protection of data and privacy for all EU citizens and those in the European Economic Area (*GDPR*, Article 3). Under the provisions of the *GDPR*, organizations are required not only to ensure that personal data is collected lawfully and under strict conditions but also to ensure that all parties involved in data collection and management are obligated to protect the data from abuse and exploitation, as well as respect the rights of data subjects. Penalties for violations of the *GDPR* are substantial with two main types: up to 20 million euros or 4% of global turnover (whichever is higher), in addition to the right of data subjects to claim compensation for damages (*GDPR*, Article 83).

The *GDPR* is considered a significant legal advancement in defining personal data. Under the Regulation, personal data and sensitive personal data are two fundamental concepts. Accordingly, personal data is defined as any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person (*GDPR*, Article 4(1)). Meanwhile, sensitive personal data, according to the *GDPR*, is a specific set of "special categories", including genetic data, political opinions, racial or ethnic origin, data concerning health, trade union membership, religious or philosophical

beliefs, data concerning sex life or sexual orientation and biometric data (where processed to uniquely identify someone) (*GDPR*, Article 9).

The *GDPR* regulates all businesses and organizations registered in the EU, operating in the EU or having customers and users who are EU citizens (Le and Nguyen, 2020). Therefore, the *GDPR* also affects Vietnamese businesses that operate in the EU or have customers who are EU citizens. Currently, the *GDPR* is considered a reference source for developing legal frameworks related to personal data protection in many countries, such as Australia, Thailand, India and others (Chu, 2022).

When comparing the *GDPR* with Vietnam's legal provisions on personal data protection, several positive aspects of the *GDPR* can be identified as references for Vietnam, including:

- Personal data protection regulations are codified in a unified legal document (the *GDPR*), whereas in Vietnam, such provisions are scattered across various by-law documents.
- The *GDPR* provides clearer and more reasonable definitions and criteria for identifying personal data and sensitive personal data compared to Vietnamese law.
- The *GDPR* establishes principles for personal data processing, serving as a crucial foundation for detailing the provisions of *Law on Personal Data Protection*.
- The penalties under the *GDPR* are more deterrent than those under Vietnamese law. While Vietnam's maximum fine is approximately 3,000 euros, the *GDPR* imposes fines of up to 20 million euros or 4% of global revenue, whichever is higher.

3.2 The *Budapest Convention*

According to the *Budapest Convention*, the following crimes pertain to the infringement of personal data in cyberspace:

Illegal access (Article 2)

"Illegal access" is understood as intentionally accessing all or part of a computer system without proper authorization. These actions may alter or damage computer systems and data. Furthermore, illegal access to computer systems can enable the actor to gain access to sensitive data (such as passwords), which may then lead to the theft of data stored in the system, including personal data (Council of Europe, 2001).

Data interference (Article 4)

This refers to a situation where an unauthorized person intentionally damages, deletes, alters or prevents access to computer data, including personal data stored in computer systems. These actions hurt the accuracy and integrity of the computer data stored in the system, making it impossible or ending for authorized users to get to the data from the computer system or other devices that hold the data.

Computer-related forgery (Article 7)

This refers to an act of an unauthorized person intentionally inserting, replacing, deleting or compressing computer data in such a way that the data becomes inaccurate, with the intention that this data will be considered or used for lawful purposes as if it were genuine, regardless of whether the data can be directly read or recognized.

Computer-related fraud (Article 8)

Computer-related fraud refers to the act of an unauthorized person intentionally causing harm to another person's property by inserting, altering, deleting, compressing computer data or engaging in any other action that disrupts the operation of a computer system with the intent to deceive or act dishonestly to illegally gain economic benefits for themselves or others.

Offences related to child pornography (Article 9)

According to Article 9(2) of the Convention, "child pornography" includes pornographic material that visually depicts a minor engaged in sexually explicit conduct, a person appearing to be a minor engaged in sexually explicit conduct, or realistic images representing a minor engaged in sexually explicit conduct. Under Article 9(1) of the Convention, offences related to child pornography are acts committed by unauthorized persons intentionally, including producing child pornography for the purpose of its distribution through a computer system, offering or making available child pornography through a computer system, distributing or transmitting child pornography through a computer system, procuring child pornography through a computer system for oneself or for another person or possessing child pornography in a computer system or on a computer-data storage.

Criminal liability of legal entities (Article 12)

According to Article 12 of the *Budapest Convention*, a legal entity may be held criminally liable for acts of crime specified in the Convention if the following conditions are met:

- An individual commits a criminal act for the benefit of a legal entity;
- The individual committing the crime is a representative or an employee of the legal entity and holds a leadership position.

Compared to the provisions of the *PCV*, the regulations in the *Budapest Convention* on crimes related to personal data breaches have certain advantages, including:

- The legislative technique in the *Budapest Convention* is more reasonable, as it only provides a general outline of the elements of the crime. The Convention's explanatory report provides a detailed description of the legal characteristics of each crime. In contrast, the approach in the *PCV*, which lists specific objective elements of crimes in detail, is ineffective and outdated compared to the evolving methods of addressing such crimes in practice.
- The *Budapest Convention* includes provisions on crimes related to child pornography and the criminal liability of legal entities, which are not present in the *Penal Code* of Vietnam. Notably, the *United Nations Convention on Cybercrime* also includes similar provisions to those in the *Budapest Convention* (*UN Convention on Cybercrime*, Articles 14 and 18).

4. Findings and recommendations

To improve Vietnam's criminal law regarding the protection of personal data in cyberspace, it is essential to refer to the provisions in the *GDPR* and the *Budapest Convention* related to these matters, partly relying on the analysis in previous sections. On that basis, the following recommendations on short- and long-term legal reforms are proposed.

- 1) Regarding short-term legal reform, the *PCV* should be amended and supplemented, including:
 - a) Legislative techniques regarding crimes related to personal data violations in cyberspace in the *PCV* should be revised. Due to the

rapid development of science and technology, the *PCV* should not list specific criminal acts in detail related to personal data violations in cyberspace; instead, it should only outline the legal characteristics of these crimes. The *Budapest Convention*, for instance, only provides a general outline of the criminal signs, and the detailed legal characteristics of each crime are described in its explanatory report. As a result, the *PCV* should only describe in broad terms the legal signs of crimes involving the violation of personal data in cyberspace. Meanwhile, a detailed description of the specific objective acts or methods of committing the crimes should be outlined in legal guidance documents.

- b) Provisions on crimes related to online child sexual abuse or child exploitation materials should be supplemented in the *PCV*. Vietnam has yet to provide a definition of child sexual abuse materials in line with international standards and has not criminalized certain acts related to online child sexual abuse or child exploitation materials. Meanwhile, international legal frameworks, including the *Budapest Convention*, have long addressed these issues. Therefore, it is essential to refer to the *Budapest Convention* to supplement the definition and criminalize acts related to online child sexual abuse or child exploitation materials in the *PCV*.
 - Child sexual abuse material refers to material in various forms, such as images, videos, audio or any other recording or depiction that realistically portrays acts of sexual abuse and/or focuses on the genitalia of children.
 - Criminal acts related to online child sexual abuse or child sexual exploitation materials include producing, offering, selling, distributing, transmitting, broadcasting, displaying, publishing or otherwise making available child sexual abuse or child sexual exploitation material in cyberspace; soliciting, procuring or accessing child sexual abuse or child sexual exploitation material in cyberspace; and possessing or controlling child sexual abuse or child sexual exploitation material stored in an information and communications technology system or another storage medium.
- c) Provisions regarding the criminal liability of legal entities for crimes related to the violation of personal data in cyberspace

should be added to the *PCV*. According to the *Budapest Convention*, legal entities can be charged with a crime when someone breaches personal data while working for or on behalf of the legal entity. This person is considered an agent of the legal entity and is therefore criminally responsible. In contrast, according to the provisions of the *PCV*, the subjects of these crimes can only be individuals. In practice, there have been many cases of personal data violations in Vietnam, such as illegal collection, illegal sale and unauthorized public disclosure, carried out by legal entities. However, since the *PCV* does not recognize legal entities as subjects of such crimes, they only face administrative or civil liability. Therefore, referencing the provisions of the *Budapest Convention* provisions on the criminal liability of legal entities ensures compatibility with international legal standards and aligns with Vietnam's practical situation.

These recommendations are feasible as they align with the provisions of the *United Nations Convention against Cybercrime*, in which Vietnam has actively participated in the drafting process. Moreover, they are consistent with the policy of amending and supplementing the *PCV* in the near future.

- 2) As to long-term legal reform, the *Law on Personal Data Protection* should be enacted to create a comprehensive and unified legal framework for personal data protection. A common legal framework for personal data protection is the foundation for improving the provisions of the *PCV* regarding crimes related to personal data protection in cyberspace. The *Law on Personal Data Protection* should be based on the current provisions of 'Decree No. 13/2023/ND-CP' and by referencing the provisions in the *GDPR*. The *GDPR* has an increasing global impact and is considered a reference for establishing legal environments related to personal data protection in many countries. Therefore, it is essential to consult the provisions of the *GDPR* when drafting the Vietnamese *Law on Personal Data Protection*. The key aspects of the *GDPR* that should be considered include defining personal data and sensitive personal data, data processing principles and penalties for individuals, businesses and organizations that violate personal data protection provisions. The challenge in implementing this recommendation is that Vietnam has up to 69 legal documents directly related to "personal data", issued by various authorities. Therefore, a unified coordination among these authorities is required in drafting and promulgating the *Law on Personal Data Protection*.

5. Conclusion

Personal data is fundamental to an individual's identification and privacy. Safeguarding this information is essential to avert misuse and to guarantee personal protection. In the absence of adequate safeguards, personal data may be susceptible to dangers such as identity theft and fraud. In fact, personal data violations in cybercrime in Vietnam have recently become more serious but law enforcement is still ineffective. In the context that the provisions in the *GDPR* and the *Budapest Convention* are crucial legal standards, Vietnam should refer to them in the process of improving its criminal laws regarding crimes related to personal data violations in cyberspace. The compatibility between Vietnamese law and European Union law will contribute to ensuring the effective prosecution of crimes involving personal data breaches in cyberspace, as well as safeguarding information security and the human rights of citizens in Vietnam and EU Member States.

Dr **Nguyen Thi Anh Hong** is head of the Department of Criminal Law at Ho Chi Minh City University of Law. She is a member of the Law Expert Society of Ho Chi Minh City University of Law and Vietnam Law Expert Society. From 2004–2011, she participated in the work of People's Juror at the People's Court of Ho Chi Minh City. Her research activities are related to criminal legal science and human rights and include the compilation of many monographs, textbooks and study materials. Dr Nguyen Thi Anh Hong is the author and co-author of many scientific works covering research topics at all levels. The author's main research interests focus on criminal law issues, especially non-custodial penalties.

Dr **Tran Thanh Thao** is a lecturer of law at the Faculty of Criminal Law at Ho Chi Minh University of Law. He has written and published domestic and international articles and seminary papers in Vietnam as well as monographs and textbooks on criminal law, published in Vietnam over the years. He has been the principal investigator and member of research projects at all levels, including 'Limiting the death penalty in Vietnam's criminal law' (a university-level research project) and 'Cybercrime in the field of information technology and telecommunication networks' (a ministry-level scientific research project). His research is mainly related to legal issues in criminal legal science, including death penalty, corruption crimes and cybercrime.

References

- Anh, M. (2024) 'Vi phạm về bảo vệ dữ liệu cá nhân vẫn diễn ra phổ biến' (Violations of personal data protection are still common), *Vietnam Lawyers Journal*. Available at: <https://lsvn.vn/vi-pham-ve-bao-ve-du-lieu-ca-nhan-van-dien-ra-pho-bien-1721139998-a145441.html> (Accessed: 22 December 2024).
- Chu, T.H. (2022) 'Personal data protection in Vietnam – Road ahead', *Vietnam Law & Legal Forum*, 7 May. Available at: <https://vietnamlawmagazine.vn/personal-data-protection-in-vietnam-road-ahead-48786.html> (Accessed: 10 December 2024).
- Convention on Cybercrime (The Budapest Convention)* (2001) T.I.A.S 131, E.T.S. No. 185. Available at: <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561> (Accessed: 6 December 2024).
- Council of Europe (2001) *Explanatory report to the Budapest Convention*. Available at: <https://rm.coe.int/16800cce5b> (Accessed: 6 December 2024).
- 'Decree 13/2023/ND-CP on Personal Data Protection' (2023) Government of Vietnam. Available at: <https://vietanlaw.com/decreed-13-2023-nd-cp-on-protection-of-personal-data/> (Accessed: 17 December 2024).
- de Terwangne, C. (2021) 'Council of Europe Convention 108+: a modernised international treaty for the protection of personal data', *Computer Law & Security Review*, 40, article 105497. <https://doi.org/10.1016/j.clsr.2020.105497>
- ECPAT, INTERPOL and UNICEF (2022a) *Disrupting harm in Vietnam [Snapshot]: evidence on online child sexual exploitation and abuse*. Reliefweb. Available at: <https://reliefweb.int/report/viet-nam/disrupting-harm-viet-nam-snapshot-evidence-online-child-sexual-exploitation-and-abuse-envi> (Accessed: 17 November 2024).
- ECPAT, INTERPOL and UNICEF (2022b) *Legislation addressing online child sexual exploitation and abuse*. End Violence Against Children. Available at: <https://safeonline.global/wp-content/uploads/2023/12/Disrupting-Harm-Data-Insight-4-Legislation-addressing-OCSEA.pdf> (Accessed: 27 November 2024).
- European Data Protection Supervisor (2018) *The History of the General Data Protection Regulation*. Available at: https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (Accessed: 27 November 2024).
- Framework Agreement on Comprehensive Partnership and Cooperation between the Socialist Republic of Vietnam and the European Union and its member states* (2012). Available at: <https://eur-lex.europa.eu/EN/legal-content/summary/eu-vietnam-framework-agreement-on-comprehensive-partnership-and-cooperation.html> (Accessed: 13 November 2024).

- Ministry of Information and Communications (Vietnam) (2022) 'Mua bán dữ liệu cá nhân trên mạng dễ dàng' (Buying and selling of personal data online is easily accessible), 1 June. Available at: <https://mic.gov.vn/mua-ban-du-lieu-ca-nhan-tren-mang-de-dang-197152958.htm> (Accessed: 30 November 2024).
- Ministry of Public Security (Vietnam) (2024) *Report No. 155/2024/TTr-BCA dated 04 April 2024 on Law on Personal Data Protection formulation proposal*. Hanoi: Ministry of Public Security.
- Nguyen, T.P.H. and Tran, T.T. (2024) 'Shortcomings in the regulations of criminal law on cyber crime and recommendations', *VNU Journal of Science: Legal Studies*, 40(3). Available at: <https://doi.org/10.25073/2588-1167/vnuls.4557>
- People's Court of Phu My (2022) Judgment No. 30/2022/HS-ST on the crime of raping a person under 16 years old, Ba Ria-Vung Tau Province.
- Quan, H. (2024) 'Nguy cơ bùng phát các loại tội phạm liên quan đến dữ liệu cá nhân' (Risk of outbreak of crimes related to personal data), *Public Security News*. Available at: <https://cand.com.vn/Cong-nghe/nguy-co-bung-phat-cac-loai-toi-pham-lien-quan-den-du-lieu-ca-nhan-i733556/> (Accessed: 24 December 2024).
- 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)' (2016) *Official Journal*, L 119, 4 May. Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (Accessed: 23 November 2024).
- Supreme People's Court (Vietnam) (2024) *Statistical report on trial data from 2018 to 2024*. Available at: <https://congbobanan.toaan.gov.vn/6tatcvn/Thong-ke> (Accessed: 29 January 2025).
- The *Penal Code (Vietnam) 2015* (2017) No. 100/2015/QH13. Available at: <https://www.wipo.int/wipolex/en/legislation/details/17225> (Accessed: 17 December 2024).
- Tran, T.V.H. (2024) 'Pháp luật quốc tế về bảo vệ dữ liệu cá nhân và gợi mở cho Việt Nam' (International law on personal data protection and suggestions for Vietnam), *Human Rights and Life*, 29 June. Available at: <https://www.xaydungdang.org.vn/nhan-quyen-va-cuoc-song/phap-luat-quoc-te-ve-bao-ve-du-lieu-ca-nhan-va-goi-mo-cho-viet-nam-21130> (Accessed: 15 December 2024).
- Tropp, E.-M., Hoffmann, T. and Chochia, A. (2022) 'Open data: a stepchild in e-Estonia's data management strategy?' *TalTech Journal of European Studies*, 12(1), pp. 123–144. <https://doi.org/10.2478/hjes-2022-0006>.
- Van, T. (2022) 'Bắt nhóm đối tượng mua bán trái phép hơn 6,2 triệu dữ liệu cá nhân' (Arrest of a group of subjects illegally buying and selling more than 6.2 million personal data), *SGGP News*. Available at: <https://www.sggp.org.vn/bat-nhom-doi-tuong-mua-ban-trai-phiep-hon-62-trieu-du-lieu-ca-nhan-post624124.html> (Accessed: 15 December 2024).

Zolkin, V., Chochia, A. and Hoffmann, T. (2023) 'Automated decision-making in the EU Member State's public administration: the compliance of automated decisions of the Estonian Unemployment Insurance Fund with Estonian administrative procedure law', *European Studies – The Review of European Law, Economics and Politics*, 10(2), pp. 178–202. <https://doi.org/10.2478/eustu-2023-0017>.