International Journal of Multidisciplinary Research and Development
www.allsubjectjournal.com
ISSN Online: 2349-4182 ISSN Print: 2349-5979
Received: 20-10-2025, Accepted: 19-11-2025, Published: 04-12-2025
Volume 12, Issue 12, 2025, Page No. 24-28

Human security from the perspective of ensuring personal information security in the digital age in Vietnam

Nguyen Thi Que Loan[1*], Tran Thi Hoai Linh[2]
[1] Associate professor, Faculty of Early Childhood Education, Thai Nguyen University of Education, Vietnam
[2] Faculty of Foreign Languages, Thai Nguyen University of Education, Vietnam

Abstract
Cyberspace offers many benefits but also poses challenges to personal information security. This article examines the current state of personal information security in Vietnam and the risks in the digital technology context, thereby proposing solutions to protect personal data. The study uses qualitative methods to analyze secondary documents published on Vietnam's official news websites and legal documents regulating technology and technological security. The results show that personal information security in Vietnam is complex, requiring the involvement of the government and individuals in managing and using social networks and protecting data. Raising awareness, improving policies, and applying security technologies are necessary to limit risks and ensure personal information security in the digital age.

Keywords: Safety, assurance, personal information security, digital technology, solutions

Introduction

Over the past two decades, the use of the Internet for community connectivity has grown rapidly. In particular, the COVID-19 pandemic and social distancing policies have accelerated the digital transformation in various fields, providing people with many opportunities for learning and interaction. Alongside the many benefits it brings, cyberspace can also increase the risk of negative experiences, including personal information security issues. If personal information data is leaked, exposed, or stolen, it can not only cause material and mental losses but also endanger the life of the individual (Öğütçü *et al*., 2016) [14]. Therefore, ensuring personal information security is one of the aspects related to ensuring human security in the digital age, aiming to avoid the consequences and risks of personal data security breaches.

This article aims to explore the issue of human security from the perspective of personal information security in the digital age. The following research questions are discussed in the article: (1) what is the current state of personal information security in Vietnam? (2) What are the causes of personal information security breaches, and (3) how can personal information security be ensured in the online environment?

In terms of content, the study focuses on ensuring personal information security (personal data protection, privacy, and data abuse prevention) as a component of human security.

In terms of timeframe, the study covers the period from 2016 to the present, aligning with the process of promoting national digital transformation, particularly following the issuance and implementation of Decree No. 13/2023/NĐ-CP on personal data protection.

Methods and research data

Our study uses qualitative methods to analyze Vietnamese legal texts and state policies related to personal data protection; typical cases of personal information leaks or misuse; general cyber security threats, particularly those involving personal information when using social media; and the consequences of personal information security breaches.

This study only uses secondary data obtained from publicly available articles on Vietnam's official news websites or official legal documents and does not collect any personal information or sensitive information.

Research Findings

1. General Issues Regarding Personal Information Security in Vietnam

- **Security:** In its simplest sense, it means "the ability to maintain safety in the face of threats" (Gasper & Gómez, 2015; NCQT, 2014a) [5, 9] or refers to "a state of stability, safety, without signs of danger or threats to the normal existence and development of individuals, organizations, specific areas of social activity, or society as a whole" (NCQT, 2014b) [10].

The concept of security can be viewed from two perspectives: (i) the social perspective, which is the peaceful state or condition of a community or nation; (ii) the individual perspective, which is the psychological state of peace of mind for individuals, free from threats or dangers to their happiness or life. While the goal of national security is to protect the state from external threats, the focus of human security is to protect individuals from threats to their happiness and existence (Holliday & Howe, 2011) [7].

- **Human security:** The concept of human security began to gain recognition when it was introduced as a theme in the United Nations' 1994 [19] "Human Development Report," which defined human security is "safety from the constant threats of hunger, disease, and oppression, as well as protection from sudden and harmful disruptions to daily life patterns- whether at home, at work, or in the community". Human security threats are viewed through seven fundamental issues: (i) economic security, (ii) food security, (iii) health security, (iv) environmental security, (v) personal security, (vi) community security, and (vii) political security (United Nations, 1994) [19]. This people-centered concept

quickly gained widespread support and attracted the attention of many scientists researching human security from different perspectives, including the issue of personal information security.

- **Information security and ensuring information security:** Article 3, Clause 24 of Decree 72/2013/NĐ-CP on "Management, provision, and use of Internet services and information on the network" stipulates that "Information security is ensuring that information on the network does not harm national security, social order and safety, state secrets, or the legitimate rights and interests of organizations and individuals" (Hama, 2017; Decree 72/2013/ND-CP on Management, Provision, and Use of Internet Services and Information on the Network, n.d.) [6]. According to the Ministry of Information and Communications - Ministry of Public Security, ensuring information security refers to "activities of managing, controlling, preventing, detecting, blocking, and combating acts of using or exploiting postal, telecommunications, and information technology infrastructure to infringe upon national security, social order and safety, and the interests of citizens." (Point b, Clause 2, Section 1) (Joint Circular 06/2008/TTLT-BTTTT-BCA on Ensuring Infrastructure Safety and Information Security in Postal, Telecommunications, and IT Activities, n.d.).).

- **Personal Information:** According to Decree No. 64/20 07/NĐ-CP, personal information is understood to be "information sufficient to accurately identify an individual, including at least the following: full name, date of birth, occupation, title, contact address, email address, telephone number, national identification number, passport number. Personal confidential information includes medical records, tax records, social security card numbers, credit card numbers, and other personal secrets" (Conger *et al*., 2013; "(Decree 64/2007/NĐ-CP Application of Information Technology in State Agencies Latest, n.d.) [3].

Personal information is further specified in Decree No. 13/2023/NĐ-CP (Article 2) (thuvienphapluat.vn, 2025) [17] that is "information in the form of symbols, letters, numbers, images, sounds, or similar forms in an electronic environment associated with a specific person or helping to identify a specific person" (paragraph 1, Article 2). Personal information is categorized into basic personal data (Article 2, Clause 3), which includes: Full name, date of birth, gender, nationality, personal image, telephone number, national identification number, vehicle registration number, tax code, account number, marital status, family relationships, etc. and sensitive personal data (Article 2, Clause 4), including: political views, religious views; health status, private life recorded in medical records; information related to racial origin, ethnic origin; information about an individual's sex life, sexual orientation; data on an individual's location determined through location services; customer information of credit institutions.

- **Ensuring personal information security:** From the concepts mentioned above, ensuring personal information security can be understood as "activities to manage, control, prevent, detect, stop, and combat acts of using and exploiting citizens' personal information to violate their security and interests".

2. Current state of personal information security in Vietnam

In recent years, rapid development at low cost has led to an explosion in the number of Internet users in Vietnam. According to statistics from the Vietnam Network Emergency Response and Security Center (VNETWORK), as of early 2024, Vietnam's population reached 101,112,656 people, with 78.44 million Internet users (accounting for 79.1% of the total population); including 72.70 million social media users (73.3% of the total population); and 168.5 million active mobile connections (169.8% of the total population) (Digital Statistics in Vietnam 2024 You Need to Know, n.d.). These figures show that Vietnam has a significant total number of Internet, social media, and mobile users. This also means an increased risk to personal information security- especially as sharing personal information on online platforms becomes easier and more common when individuals use online transactions, e-commerce, and e-banking. They must disclose information such as: name, date of birth, contact address, phone number, ID number/national ID card number. In the digital age, this personal information has become a target and valuable asset for many parties to collect, store, analyze, and exploit for various purposes. If this information is not protected, it can be collected and exploited illegally by bad actors, causing financial losses; causing frustration, irritation, stress, and anxiety; and loss of trust in companies and organizations that violate personal data security. Therefore, based on the actual situation in Vietnam, the State has issued many legal documents to manage, control, prevent, and combat the use and exploitation of personal information to violate the security and interests of citizens, notably the following documents (Table 1).

Table 1: Selected legal documents related to personal information security

No.	Issuing Authority	Name of Document	Date of Issuance	Content related to personal information security
1.	National Assembly	Information Technology Law (thuvienphapluat.vn, 2025b)	June 29, 2006	Articles 21, 22
2.	National Assembly	Telecommunications Law (thuvienphapluat.vn, 2025f)	November 24, 2023	Article 6
3.	National Assembly	Constitution of the Socialist Republic of Vietnam (Constitution of the Socialist Republic of Vietnam 2013, n.d.)	November 28, 2013	Article 21
4.	National Assembly	Cybersecurity Law (Government, n.d.)	November 19, 2015	Chapter I: Article 4, Article 7; Chapter II: Section 2
5.	National Assembly	Civil Code (Civil Code 2015 No. 91/2015/QH13 Effective 2025 Latest, n.d.)	November 24, 2015	Article 38
6.	National	Cybersecurity Law (LuatVietnam, n.d.)	June 12, 2018	Article 8, Section 5; Article

	Assembly			17
7.	National Assembly	Consumer Protection Law (thuvienphapluat.vn, 2025c)	June 20, 2024	Article 4, Section 1; Article 19
8.	National Assembly	Electronic Transactions Law (thuvienphapluat.vn, 2025e)	June 22, 2023	Article 6, Section 3
9.	Government	Personal Data Protection Decree (Decree 13/2023/ND-CP on Personal Data Protection (Latest Version, n.d.)	April 17, 2023	Full Text
10.	Government	Decree on the Management, Provision, and Use of Internet Services and Information Online (thuvienphapluat.vn, n.d.)	November 9, 2024	Full Text
11.	Ministry of Health	Decision Issuing regulations on ensuring information security and cybersecurity of the Ministry of Health (thuvienphapluat.vn, 2025d)	July 12,2024	Full Text
12.	Ministry of Home Affairs	Decision Issuing the Regulations on Ensuring Information Security and Cybersecurity of the Ministry of Home Affairs (thuvienphapluat.vn, 2025g)	July 10, 2025	Full Text

Source: Compiled by the author

All of the above documents contain specific provisions on personal information protection to ensure personal privacy; strictly prohibit organizations and individuals from illegally collecting or exploiting personal information for the purpose of sabotage or illegal profit; and require organizations and individuals to implement appropriate measures to protect personal information. For individuals and organizations that use personal information illegally, the Civil Code, Information Technology Law, Consumer Protection Law, Electronic Transactions Law, Telecommunications Law, Personal Data Protection Decree, etc. all have legal provisions stipulating administrative or criminal liability depending on the severity of the violation by the individual or organization.

Along with activities to manage, control, prevent, detect, and combat the use and exploitation of citizens' personal information to violate their security and interests, a number of legal documents such as the Law on Network Information Security and the Decree on Personal Data Protection also clearly specify the responsibility of users to protect their own personal information and to exercise caution when providing personal information on the Internet (phủ, n.d.), because in reality, not only in Vietnam but throughout the world, the laws of all countries have provisions on the protection of personal information on the Internet. However, research by Abawajy (2014) [1] has shown that no matter how strong the legal protections and technological defenses within an organization may be, information security can still be considered the weakest link in the security chain (Abawajy, 2014) [1]. Therefore, even when using the best technology, risks to personal information security can still occur because personal data and information may be stored, processed, and copied when individuals participate as members of a website or use certain software (Acquisti, 2006) [2]. Therefore, user awareness plays a particularly important role in protecting personal information when participating in the online environment.

3. Causes of threats to personal information security

Personal information security is threatened by various causes, including the following fundamental causes:

1. Due to low awareness of personal data protection among users. Many individuals are unaware of the security risks of disclosing personal information; they carelessly and indiscriminately provide personal information when using social networks, applications, and entertainment software from untrustworthy intermediaries that lack information security policies or have poor information security policies. Therefore, by confirming information to use applications or providing images, allowing access to photo galleries, phone cameras, and other permissions, many individuals have inadvertently exposed themselves to personal information security risks.
2. Due to lax regulations on data sharing with third parties, some agencies, organizations, and businesses collect personal data and illegally share information with third parties for illicit gain or inadvertently leak information.
3. Due to vulnerabilities in the systems and applications of service providers that do not ensure cybersecurity and network security, they are susceptible to attacks and exploitation.
4. Online fraud is on the rise, with many "fake" websites created for the purpose of fraud and collecting personal information.

4. Risks and consequences when personal information security is threatened

The continued integration of technology into daily life exposes technology users to increasing risks regarding security and privacy because, to use online services, users must share their personal information such as name, date of birth, email address, phone number, citizen ID number/national ID number, etc., to verify their identity. However, in reality, many people's personal information has become a commodity traded and sold rampantly online. Simply typing the keyword "buy and sell DATA" brings up a long list of websites, Facebook pages, Telegram groups, and DATA trading groups with detailed advertisements (VnExpress, n.d.).

Personal information such as phone numbers, full names, dates of birth, personal identification numbers, household registration, service registration locations, transaction locations, savings deposits, car purchases, occupations, low-interest loans, shopping, etc., is being sold. Sellers even guarantee the accuracy of the data, commit to updating it, and offer to export data upon request. Despite the Ministry of Public Security directing law enforcement agencies to collect evidence, investigate, and prosecute numerous cases of illegal personal information trading, this practice continues unabated. According to data from the Ministry of Public Security, in early 2025 alone, 110 million personal data records were illegally collected and sold on the black market (With over 110 million personal data records being sold, citizens need to be aware of their rights, 2025) [8].

Due to the leakage of personal information, individuals impersonating police, prosecutors, or judges... use personal information to make threatening phone calls and send threatening messages, demanding that people transfer money to them or call to sell land, houses, insurance, play the stock market, provide consulting and loans, hire tutors, buy tours, etc., causing listeners to feel harassed, annoyed, or psychologically confused when threatened. By obtaining personal information, fraudsters use deepfake video calls. Using artificial intelligence (AI) technology to replicate facial features, fraudsters create fake videos impersonating relatives or friends to carry out online scam calls.

According to statistics from the Ministry of Public Security, in 2024 alone, Vietnam had more than 6,000 cases of online fraud (tra, n.d.); of which, 75% were financial fraud, and 25% were data theft for financial fraud or other malicious purposes. According to a report by the Vietnam National Cybersecurity Association, the total damage caused by online fraud in 2024 is estimated at 18.9 trillion Vietnamese doing. On average, 1 in every 220 users is a victim of online fraud, equivalent to a rate of 0.45% (National Cybersecurity Association, 2024). Common types of online fraud in Vietnam are (Table 2)

Table 2: Types of online fraud in Vietnam

E

No.	Type of fraud	Detailed Description	Recognition signs	Consequences
1	Fraud via fake messages and calls	Impersonating police, banks, or post offices to request victims to provide personal information or transfer money.	Unknown phone numbers requesting OTP codes, threatening involvement in a criminal case.	Financial loss, exposure of personal information.
2	Fake websites, online banking	Creating fake bank or e-wallet websites to steal login information.	Unfamiliar web addresses with interfaces resembling banks but containing spelling errors.	Bank account hacked, money lost.
3	Financial investment scams, cryptocurrency scams	Promising high returns, soliciting investments in cryptocurrency.	Promising large profits without clear legal information.	Loss of all invested funds.
4	Employment scam	Posting job listings with high salaries, requiring deposits or training fees.	Requiring a transfer before accepting the job.	Losing money, being tricked into joining a pyramid scheme.
5	Hacking social media accounts	Hacking Facebook and Zalo accounts, then sending messages to family members asking for money.	A familiar account sends messages asking for money but uses unusual language.	Relatives transfer money as requested and lose money unfairly.
6	Fake prize or gift scams	Notifying winners of motorcycles or phones but demanding payment upfront.	Requiring payment of fees before receiving the prize.	Losing money on fees, not receiving gifts.
7	Online shopping scams	Advertising products at low prices but failing to deliver or delivering poor-quality goods.	No clear store address, requiring payment upfront.	Losing money, receiving counterfeit goods, or not receiving goods at all.
8	Scams through loan apps	Quick loan apps with low interest rates but hidden terms, collecting personal data for blackmail.	Unclear interest rates, requiring access to your contacts.	Harassed by debt collectors, personal data lost.

Even more dangerous is the threat to children's safety when their personal data is exploited by bad actors for abuse, leading to many other consequences. Research conducted by Disrupting Harm in 13 countries, including Vietnam, on the harm caused by the leakage of children's personal information on the internet has revealed ("Disrupting Harm | End Violence," n.d.): Many cases of child bullying, abuse, and sexual exploitation originate from children having their personal information- such as names, addresses, personal photos, and private secrets-stolen online.

5. Measures to ensure personal information security

- **For individuals**

Each individual need to proactively take measures to protect their personal information, especially in the context of increasingly popular online platforms and the growing risk of data leaks. First, when using platforms or applications on smart devices, users need to be cautious about requests for personal information. Before granting access to an application, carefully consider the permissions it requests to avoid unauthorized collection of personal data. In addition, sharing personal information on social media should also be strictly controlled. Limit the disclosure of sensitive information in public, avoid posting addresses, phone numbers, or financial information to reduce the risk of exploitation by bad actors.

Furthermore, when using online services such as online banking, online shopping, or logging into personal accounts on public devices, users should ensure they log out after use. This helps prevent unauthorized access to accounts if the device falls into the wrong hands. At the same time, do not install or use software or applications from unknown sources on the Internet, as these may contain malware or spyware designed to steal personal information. Raising awareness and implementing measures to protect personal data not only helps protect privacy but also helps limit the risk of information loss, fraud, or cyber attacks.

- **For competent authorities in Vietnam**

Competent authorities in Vietnam play an important role in managing, controlling, and protecting citizens' personal information. First, it is necessary to continue implementing measures to prevent, detect, and promptly stop acts of using or exploiting personal information to violate citizens' rights and interests, affecting cybersecurity and social order. State agencies need to strengthen coordination among relevant ministries and sectors to improve the effectiveness of monitoring and handling violations. At the same time, it is necessary to develop and improve legal regulations and strict sanctions to deal with acts of personal data infringement, especially cases of illegal sale and dissemination of personal information.

Furthermore, state agencies holding citizens' personal information must take full responsibility for protecting this data, ensuring absolute security against the risks of leaks or cyberattacks. The collection, storage, and processing of personal information must strictly comply with legal regulations and apply advanced security measures to

minimize the risk of unauthorized access. Agencies are only permitted to provide or share citizens' personal data with authorized third parties when there is a clear legal basis, for the purposes of investigation, management, or other legitimate purposes in accordance with the law.

In addition, it is necessary to promote awareness campaigns to raise the awareness of individuals and organizations about their rights and responsibilities related to the protection of personal information. At the same time, it is necessary to strengthen inspection, examination, and handling of violations by units and organizations that abuse or misuse citizens' personal information. The coordinated application of these measures will contribute to building a safe and transparent digital environment that ensures the rights and interests of citizens in the digital age.

Conclusion

Threats to personal information security on the internet are constantly increasing with the emergence of new technologies and legal boundaries related to the privacy of personal information, as well as the unclear use of such information by organizations and companies. Therefore, to ensure personal information security, internet users must be aware of these threats and take effective measures to protect their personal information.

However, due to the low level of individual awareness of threats to personal information security, and the increasingly sophisticated and complex nature of high-tech crime with unpredictable developments, users still face risks of personal information security breaches when using the internet. Although Vietnam has regulations in certain laws regarding the handling of administrative or criminal violations by organisations or individuals who commit acts violating personal information security (Point b, Clause 1, Article 288 of the Criminal Code; Clause 30, Article 1 of Decree 14/2022/NĐ-CP), and most recently, the Personal Data Protection Decree, which took effect on 1 July 2023, the theft and trading of personal data online continue to occur. Therefore, it is necessary to continue improving the legal framework to promote and protect personal information security, prevent the increasingly complex situation of personal data theft, which causes serious consequences and threatens human security.

References

1. Abawajy J. User preference of cyber security awareness delivery methods. Behaviour, Information Technology, 2014:33(3):237–248. https://doi.org/10.1080/0144929X.2012.708787
2. Acquisti A. Privacy , Security of Personal Information, 2006, 179–186. https://doi.org/10.1007/1-4020-8090-5_14
3. Conger S, Pratt JH, Loch KD. Personal information privacy emerging technologies. Information Systems Journal,2013:23(5):401–417. https://doi.org/10.1111/j.1365-2575.2012.00402.x
4. Disrupting Harm End Violence. n.d. Offshore Sportsbooks. Retrieved, 2025. from https://www.end-violence.org/disrupting-harm
5. Gasper D, Gómez OA. Human security thinking in practice Personal security, citizen security comprehensive mappings. Contemporary Politics,2015: 21(1):100–116. https://doi.org/10.1080/13569775.2014.993906
6. Hama HH. State Security, Societal Security, , Human Security. Jadavpur Journal of International Relations,2017:21(1):1–19. https://doi.org/10.1177/0973598417706591
7. Holliday I, Howe B. Human Security A Global Responsibility to Protect , Provide. Korean Journal of Defense Analysis, 2011, 23.
8. With over 110 million personal data records being sold, citizens need to be aware of their rightsh, 2025. https://laodong.vn/phap-luat/hon-110-trieu-du-lieu-ca-nhan-bi-rao-ban-nguoi-dan-can-nam-ro-quyen-cua-minh-1536623.ldo
9. NCQT. Security. International Research, 2014a. https://nghiencuuquocte.org/2014/11/12/an-ninh/
10. NCQT. Security. International Research, 2014b. https://nghiencuuquocte.org/2014/11/12/an-ninh/
11. Decree No. 64/2007/NĐ-CP on the application of information technology in State agencies. (n.d.). Retrieved, 2025. from https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-64-2007-ND-CP-ung-dung-cong-nghe-thong-tin-trong-co-quan-Nha-nuoc-18234.aspx
12. Decree No. 72/2013/NĐ-CP on the management of the provision , use of Internet services , information on the network. n.d. Retrieved, 2025. from https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-72-2013-ND-CP-quan-ly-cung-cap-su-dung-dich-vu-Internet-va-thong-tin-tren-mang-201110.aspx
13. Digital figures in Vietnam for 2024 that you need to know. n.d. VIETNAM E-COMMERCE ASSOCIATION. Retrieved, 2025. from https://vecom.vn/nhung-con-so-ve-digital-tai-viet-nam-2024-ma-ban-phai-biet
14. Öğütçü G, Testik ÖM, Chouseinoglou O. Analysis of personal information security behavior , awareness. Computers Security,2016:56:83–93. https://doi.org/10.1016/j.cose.2015.10.002
15. Ministry of Information , Communications n.d. Law No. 86/2015/QH13 of the National Assembly: Law on Network Information Security. Retrieved, 2025.from http://vanban.chinhphu.vn/?pageid=27160&docid=183196
16. Joint Circular No. 06/2008/TTLT-BTTTT-BCA on ensuring infrastructure safety , information security in postal, telecommunications , information technology activities. n.d. Retrieved, 2025. from https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Thong-tu-lien-tich-06-2008-TTLT-BTTTT-BCA-bao-dam-an-toan-co-so-ha-tang-va-an-ninh-thong-tin-trong-hoat-dong-buu-chinh-vien-thong-va-CNTT-83662.aspx
17. thuvienphapluat.vn. Decree No. 13/2023/NĐ-CP on the latest personal data protection. LEGAL LIBRARY, 2025. https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-13-2023-ND-CP-bao-ve-du-lieu-ca-nhan-465185.aspx
18. Tra BT. n.d. Over 6,000 cases related to online fraud caused losses exceeding 12 trillion. Retrieved, 2025. From https://thanhtra.com.vn/an-ninh-trat-tu-D718A18CA/hon-6000-vu-lien-quan-lua-dao-truc-tuyen-gay-thiet-hai-hon-12000-ty-dong-fd59ddbc8.html
19. United Nations with UNDP. Human development report 1994. Oxford Univ. Pr, 1994.
20. VnExpress. n.d. The personal data black hole-VnExpress newspaper. vnexpress.net. Retrieved, 2025. From https://vnexpress.net/ho-den-du-lieu-ca-nhan-4623705.html.