PERSONAL DATA IN THE DIGITAL AGE: AN OVERVIEW STUDY IN VIETNAM

aLe Minh Nguyen, bLe Van Long, cTran Van Nam, dTruong Hung Chen

ABSTRACT

Purpose: In today’s era, the fourth industrial revolution, coupled with the remarkable development of information and communication technology, has shifted all human activities to the digital platform. However, personal data digitization and storage methods have risks related to data security and ensuring user privacy. This study comprehensively examines the prevailing legal framework and explores the associated challenges related to personal data protection in Vietnam.

Study methodology: Examining legal documents issued by the State is highly significant, and decrees and circulars are essential legal texts utilized in the research process. In addition to the legal bases that are considered the basis for analysis and evaluation, interdisciplinary research methods are used such as dialectical materialism methodology, analysis-synthesis, logic-history, induction-interpretation, etc.

Results and Discussion: The current legal framework on personal data protection in Vietnam has various shortcomings that must be addressed through appropriate amendments and supplements aligning with international standards. The challenges in implementing this legal framework in Vietnam must also be clarified to find solutions.

Recommendations: Securing personal data is of utmost importance because if data is stolen, it can lead to severe financial losses, the risk of extortion, fraud, asset misappropriation, defamation, infringement of dignity, honor, sexual harassment..., causing both material and psychological consequences, directly affecting the rights and legitimate interests of organizations, businesses, and individuals. Therefore, first and foremost, each needs to ensure the security of their data to prevent data theft, ensure the integrity of personal information, protect privacy rights, and avoid the consequences and risks that arise when personal data is disclosed, leaked or stolen.

Keywords: security, digital age, personal information, vietnam.

Received: 01/11/2024
Accepted: 03/04/2024
DOI: https://doi.org/10.55908/sdgs.v12i3.2623

a Master in Law, Faculty of Commercial Law, Nam Can Tho University, Cantho, Vietnam.
E-mail: leminhcantho@gmailcom Orcid: https://orcid.org/0009-0006-2244-048X
b Assoc. Prof. in Law, Dean, Faculty of Constitutional & Administrative Law, Nam Can Tho University, Cantho, Vietnam.
E-mail: vuonglonghlu@gmail.com Orcid: https://orcid.org/0000-0002-4921-6465
c Master in Information Systems, Faculty of Information Technology, Nam Can Tho University, Cantho, Vietnam.
E-mail: thchen@nctu.edu.vn Orcid: https://orcid.org/0009-0007-6177-9918
d Master in Information Systems, Faculty of Information Technology, Nam Can Tho University, Cantho, Vietnam.
E-mail: ttanam@nctu.edu.vn Orcid: https://orcid.org/0009-0008-6301-7332
DADOS PESSOAIS NA ERA DIGITAL: UM ESTUDO DE VISÃO GERAL NO VIETNÂ

RESUMO

Propósito: Na era atual, a quarta revolução industrial, aliada ao desenvolvimento notável da tecnologia da informação e comunicação, transferiu todas as atividades humanas para a plataforma digital. No entanto, a digitalização de dados pessoais e os métodos de armazenamento têm riscos relacionados à segurança dos dados e à garantia da privacidade do usuário. Este estudo examina exhaustivamente o quadro jurídico vigente e explora os desafios associados relacionados com a proteção de dados pessoais no Vietnam.

Metodologia do estudo: Examinar documentos legais emitidos pelo Estado é altamente significativo, e decretos e circulares são textos legais essenciais utilizados no processo de pesquisa. Além das bases jurídicas que são consideradas a base para análise e avaliação, são utilizados métodos de pesquisa interdisciplinares, como metodologia de materialismo dialético, análise-síntese, lógica-história, indução-interpretación, etc.

Resultados e discussão: o atual quadro jurídico sobre proteção de dados pessoais no Vietnam apresenta várias deficiências que devem ser colmatadas através de alterações e suplementos adequados, em consonância com as normas internacionais. Os desafios na implementação deste quadro jurídico no Vietnam devem também ser clarificados para se encontrarem soluções.

Recomendações: A proteção de dados pessoais é de extrema importância, pois se os dados forem roubados, podem levar a graves perdas financeiras, ao risco de extorsão, fraude, apropição indevida de ativos, difamação, violação da dignidade, honra, assédio sexual..., causando consequências tanto materiais quanto psicológicas, afetando diretamente os direitos e interesses legítimos de organizações, empresas e indivíduos. Portanto, em primeiro lugar, cada um precisa garantir a segurança de seus dados para evitar o roubo de dados, garantir a integridade das informações pessoais, proteger os direitos de privacidade e evitar as consequências e os riscos que surgem quando os dados pessoais são divulgados, vazados ou roubados.


DATOS PERSONALES EN LA ERA DIGITAL: UN ESTUDIO GENERAL EN VIETNAM

RESUMEN

Propósito: En la era actual, la cuarta revolución industrial, junto con el notable desarrollo de la tecnología de la información y la comunicación, ha trasladado todas las actividades humanas a la plataforma digital. Sin embargo, la digitalización y los métodos de almacenamiento de datos personales tienen riesgos relacionados con la seguridad de los datos y la garantía de la privacidad del usuario. Este estudio examina exhaustivamente el marco legal prevaleciente y explora los desafíos asociados relacionados con la protección de datos personales en Vietnam.

Metodología de estudio: El examen de los documentos jurídicos emitidos por el Estado es sumamente significativo, y los decretos y circulares son textos jurídicos esenciales utilizados en el proceso de investigación. Además de las bases jurídicas que se consideran la base para el análisis y la evaluación, se utilizan métodos de investigación interdisciplinarios como la metodología del materialismo dialéctico, el análisis-síntesis, la lógica-historia, la inducción-interpretación, etc.

Resultados y debate: El actual marco jurídico sobre protección de datos personales en Vietnam tiene varias deficiencias que deben abordarse mediante enmiendas y suplementos adecuados.
que se ajusten a las normas internacionales. También deben aclararse los retos que plantea la aplicación de este marco jurídico en Vietnam para encontrar soluciones.

**Recomendaciones:** Proteger los datos personales es de suma importancia porque si los datos son robados, puede provocar graves pérdidas financieras, el riesgo de extorsión, fraude, apropiación indebida de activos, difamación, violación de la dignidad, honor, acoso sexual..., causando consecuencias tanto materiales como psicológicas, afectando directamente los derechos e intereses legítimos de organizaciones, empresas e individuos. Por lo tanto, en primer lugar, cada uno debe garantizar la seguridad de sus datos para evitar el robo de datos, garantizar la integridad de la información personal, proteger los derechos de privacidad y evitar las consecuencias y riesgos que surgen cuando se revelan, filtran o roban datos personales.

**Palabras clave:** seguridad, era digital, información personal, Vietnam.

1 INTRODUCTION

The right to privacy is a part of the European Convention on Human Rights of 1950, in which it is declared that everyone has the right to respect their private and family life, home, and correspondence (Rights, n.d.). Building upon this foundation, European Union member states have sought to safeguard this right amidst the surge in information technology by creating a common legal framework. According to Juliane Kokott and Christoph Sobotta, the right to respect private life continues to be protected under the general principles of EU law (Kokott & Sobotta, 2013). Individual privacy (including data privacy) is of particular concern and is regulated through the overarching provisions of the GDPR that apply to member states.

In Vietnam, human rights and personal privacy, including personal data, are safeguarded through specific regulations. Article 21 of the 2013 Constitution of Vietnam stipulates that everyone has the right to inviolability of personal life, personal secrets, and family secrets, and the right to protect their honor and reputation. The law ensures the safety of information related to personal life, personal secrets, and family secrets. However, with the rapid pace of the Fourth Industrial Revolution (The Industrial Revolution 4.0 or The Fourth Industrial Revolution 4IR), a term describing the rapid changes in technology, industries, and society in the 21st century characterized by increased connectivity and intelligent automation through the Internet of Things (IoT), real-time data access, and the introduction of smart technology systems, Industry 4.0 aims to create efficient management processes in various social aspects, including the management of personal data. Digital personal data, stored and managed online, offers many advantages such as easy accessibility, time and effort savings, and ease of
information sharing. Nevertheless, this data is vulnerable to breaches and exploitation for various purposes by third parties. Therefore, establishing comprehensive legal frameworks in each country to protect personal data is essential to prevent the exploitation and misuse of personal data, safeguard the rights and interests of data subjects, and prevent negative impacts on human security.

2 THEORETICAL FRAMEWORK

Across the world, safeguarding personal data has become a significant priority for many countries and organizations. More than 80 countries, including the United States, France, Germany, Japan, and the European Union (EU), have implemented legal regulations to protect this right. Nations view the protection of personal data as a crucial aspect of privacy, ensuring its safeguarding by law. Protecting personal data manifests as an assurance of individual autonomy, privacy, and the preservation of each individual's dignity and reputation. This enables individuals to exercise better control over various aspects of their lives, fosters increased trust within society, and plays a vital role in promoting freedom of speech and the expression of one's views. In Vietnam, the objective of protecting personal data is to ensure the safety, security, and privacy of individuals' personal information. To achieve this goal, Vietnam has implemented a series of measures, including the enactment of regulations and laws related to personal data protection. However, safeguarding users' data has become a growing concern in the digital technology era. This article provides an overview of the regulations for personal data protection in Vietnam and offers some solutions to ensure that Vietnamese citizens have the right to freely and securely share their personal information without it being abused or infringing on their privacy.

3 MATERIAL AND METHODS

Due to the exploratory nature and context of the research, a qualitative research design is employed. The qualitative research method allows for an in-depth investigation into the phenomenon under study. The research design encompasses an initial phase that focuses on document analysis, including policies in compliance with GDPR and Vietnamese legal documents regulating personal data security and protection.
mechanisms, as well as sanctions for unauthorized breaches of personal data. Furthermore, the article utilizes legal writing analysis, logical methods, systematic organization, analysis, synthesis, and accurate evaluation of information and data as a basis for solutions concerning personal data protection in the digital age.

4 RESULTS AND DISCUSSIONS

4.1 COMMON ISSUES REGARDING PERSONAL DATA IN THE DIGITAL AGE

Personal data security according to GDPR: The GDPR content consists of 11 Chapters and 99 Articles, focusing on the following topics: the scope of regulation; principles related to the processing of personal data; Rights of data subjects; rights and obligations of data controllers and data processors; transfer of personal data to a third country or international organizations; competent supervisory authorities; remedial measures; legal liabilities and forms of sanctions for breaches and enforcement mechanisms.

GDPR is considered a significant legal milestone in defining personal data. Personal data and sensitive personal data are fundamental concepts within GDPR. As per GDPR, personal data refers to any information relating to an identified or identifiable natural person (data subject). According to the GDPR, personal data refers to any information related to an identified or identifiable natural person (data subject). An identifiable natural person is someone who can be directly or indirectly identified, particularly by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more specific factors related to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. (GDPR.EU, n.d.). In other words, personal data (also known as private data) is information about a specific individual that can be used to identify or contact that person. This encompasses a range of information such as names, addresses, phone numbers, email addresses, date of birth, identity numbers, passports, and many other types of data. Personal data can also include information like images, fingerprints, medical records, financial history, and other details that can be used to identify or contact a specific person. According to GDPR's explanation, a person can be directly identified when the identification can be made solely based on the information at hand. Indirect identification,
on the other hand, occurs when identification cannot be made from the available information, requiring additional information from other sources. Therefore, even information that is explicit or in some cases, doesn't contain the individual's name but helps to understand or has an impact on an individual, may be considered personal data. (GDPR.EU, n.d.).

GDPR distinguishes between personal data and sensitive personal data. Sensitive personal data is defined under GDPR as a category of special personal data, considered to be any data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic or biometric data to uniquely identify a person, or data concerning health, sex life, and sexual orientation. Moreover, security is considered a state of being free from threats, addressing the safety of a nation, organization, or individual. Security also refers to measures implemented as prescribed to ensure safety, guarding against external threats that may harm the protected entities. In line with this perspective, the author Emma Rothschild argues that security is about safety and necessitates measures to mitigate and address threats (Rothschild, 1995).

As regulated by GDPR, personal data security means safeguarding users' privacy and personal information from unauthorized access, use, or disclosure. Personal data includes any information related to a specific individual that can be used to identify or contact them, such as names, addresses, phone numbers, email addresses, dates of birth, personal identification numbers, financial information, and various other types of data. Protecting personal data security is integral to ensuring individuals' privacy rights, as GDPR prescribes.

GDPR also outlines measures for protecting personal data, including establishing a permanent body (composed of member state representatives within GDPR) tasked with data protection at the Union level. This body is responsible for guiding GDPR implementation, advising the European Commission on personal data privacy issues, and resolving disputes between national authorities. Additionally, the European Commission appoints a dedicated leader responsible for monitoring the enforcement and application of data protection regulations within the European Union's institutions (Protection, n.d.).

The measures specified in the chapters of GDPR include regulations regarding the rights and obligations of data controllers and data processors, provisions for the transfer of personal data to third countries or international organizations, competent supervisory
authorities, remedial measures, legal responsibilities, forms of sanctions, and enforcement mechanisms. Under GDPR provisions, aimed at preventing and addressing violations of personal data, this means breaches of security that lead to the accidental or unlawful destruction, loss, alteration, disclosure, or unauthorized access to personal data transmitted, stored, or processed in other ways. Within the mechanisms for personal data protection, GDPR recognizes the rights and obligations of the parties involved, as follows:

**GDPR provisions on the rights of data subjects:** Article 13 of the GDPR stipulates that data subjects have the right to be informed about the collection and use of their data (right to be informed). Data controllers are obliged to provide information about the purposes of processing personal data, the duration of data retention, and the recipients to whom the data may be disclosed. Data subjects also have the right to access their data (right to data access); Article 15 of the GDPR, data subjects have the right to receive confirmation from the data controller about the processing of their data. Article 16 grants data subjects the right to rectify inaccurate data and request the erasure of data (right to erasure or right to be forgotten) in certain cases. Article 18 empowers data subjects to restrict the use of their data in some instances, including the right to temporarily transfer selected personal data to another processing system, making the chosen personal data temporarily unavailable to users, or temporarily removing disclosed personal data from a website. Additionally, under Articles 20 and 21 of the GDPR, provisions regarding the rights of data subjects include the right to receive the data they have provided to the data controller and request the transfer of this data to another data controller, without hindrance from the data controller currently in possession of their data when the request is made. In specific situations, data subjects also have the right to object to the processing of their data.

The GDPR provisions regarding the obligations and responsibilities of data controllers and data processors are outlined in Articles 24 through 43. These articles detail the fundamental responsibilities of the parties involved in controlling and processing personal data, with severe penalties, such as those specified in Article 83. The maximum fine can amount to 20 million Euros or 4% of the company's global annual revenue (for the preceding 12 months) in the event of a violation.

Regarding the obligations of the data controller under GDPR, it is stipulated that the data controller must establish appropriate and effective measures to protect personal
data, demonstrating their compliance and effectiveness with GDPR requirements (Article 24 GDPR). In addition, GDPR also outlines the duties and responsibilities of entities involved in the processing of personal data, such as data controllers, data processors, and designated data protection officers within organizations. Both data controllers and data processors must take steps to ensure that any individuals acting under the authority of the data controller or data processor do not process the data except on instructions from the data controller unless required to do so by the supervisory authority or the law of the Union or the Member State (Article 32 GDPR).

The processing and analysis of sensitive data are entirely prohibited under GDPR. Some exceptions permit processing sensitive personal data, including obtaining the data subject's explicit consent, protecting vital interests, preventive or occupational medicine, or for reasons of substantial public interest.

Vietnam's Personal Data Policy in the Digital Age: The policy on safeguarding personal data in the digital age is a crucial component of ensuring user privacy and data security. Vietnam has taken measures to enhance personal data protection in the context of the rapidly evolving information technology landscape. According to Datareportal statistics, there were 77.93 million internet users in Vietnam at the beginning of 2023, with an internet penetration rate of 79.1%. Vietnam is home to 70 million social media users as of January 2023, accounting for 71.0% of the total population. In early 2023, there was a total of 161.6 million active mobile connections in Vietnam, equivalent to 164.0% of the total population (Datareportal, 2023). In response to this situation, Vietnam has issued various documents to regulate the protection of personal data in the digital age.

The regulation of personal data (or personal information) in Vietnam is governed by various legal documents specific to each field. However, detailed provisions are laid out in the 2018 Cybersecurity Law, where the state employs measures to safeguard the national cyberspace, prevent and address activities that infringe upon national security, public order, social safety, as well as the lawful rights and interests of organizations, individuals on cyberspace (Article 6). In addition, a noteworthy legal document is Decree No. 13/2023/NĐ-CP, which governs the protection of personal data, passed by the Vietnamese National Assembly and effective from July 1, 2023 (Decree 13). Notable policies on personal data protection in this decree include: Personal data is processed in accordance with legal regulations; Data subjects are informed of activities related to the processing of their personal data, except where the law provides otherwise; Personal data
is only processed for the purposes specified by the data controller, data processor, data controller and processor's representative, or a third party, and the collected personal data must be appropriate and limited to the scope of the necessary processing; Personal data cannot be bought or sold under any circumstances, except where the law provides otherwise; Personal data must be updated and supplemented as necessary for processing purposes; Personal data is subject to protection and security measures during processing, including protection against violations of personal data protection regulations and prevention of loss, destruction, or damage due to incidents, using technical measures; Personal data is only stored for a reasonable period in accordance with the purposes of data processing, except where the law provides otherwise; Data controllers and processors must comply with the principles of data processing as specified and demonstrate their compliance with these principles; These policies aim to strengthen the protection of personal data and ensure responsible data processing in Vietnam.

The regulations on personal data protection under Decree 13 highlight the significant concern of the Vietnamese Government for safeguarding personal data. These provisions align with GDPR (General Data Protection Regulation); however, Vietnamese law includes exceptions where the disclosure of personal information is required in certain circumstances: Firstly, in the interest of national security and public safety, the government may demand the provision of personal information to safeguard national security or public safety. Secondly, government authorities or state management agencies may request the disclosure of personal information to fulfill their management duties, such as tax audits, border management, or the execution of social programs. Thirdly, in cases of urgent health emergencies, personal information may be disclosed to provide assistance to patients or to mitigate risks to public health. Apart from the situations outlined above, other regulations may apply, as stipulated in various laws, government decrees, or other state management agencies, which may require the disclosure of personal information.

The regulations on exceptions in Vietnamese law are in alignment with the provisions of the GDPR. As outlined in Article 23 of GDPR, similar exceptions are specified, where the provision of personal data is necessary for the protection of national security, defense, the prevention, investigation, detection, or prosecution of criminal offenses, including the protection and prevention of threats to public security, important objectives for the common interests of the Union or a Member State, particularly
economic or financial interests of the Union or a Member State, including monetary, budgetary, and tax matters, public health, and social security; safeguarding the independence of the judiciary and judicial proceedings, the prevention, investigation, detection, and prosecution of breaches of professional ethics for regulated professions... These exceptions in both Vietnamese law and the GDPR are designed to address circumstances where the safeguarding of important public interests or the functioning of justice and legal proceedings justifies the processing of personal data, even in cases where it would otherwise require consent or fall under the scope of data protection regulations.

Furthermore, by the provisions of the 1950 European Convention on Human Rights, exceptions are also stipulated for the provision of personal data. According to this convention, authorities shall not interfere with the exercise of this right except as provided by law and as necessary in a democratic society in the interests of national security, public safety, the economic well-being of the country, the prevention of disorder, and crime, for the protection of health or morals, or the protection of the rights and freedoms of others (Echr, n.d.).

Vietnamese law also establishes enforcement mechanisms to safeguard the rights of personal data owners, with prohibited actions outlined in Article 8 of Decree 13. These prohibited actions include processing personal data in violation of legal regulations concerning personal data protection, processing personal data to create information or data that opposes the Socialist Republic of Vietnam, processing personal data to create information or data that adversely affects national security, public order, social safety, or the lawful rights and interests of other organizations and individuals.

The rights of data subjects are categorized as defined in Article 9 of Decree 13, including The right to know: Data subjects have the right to be informed about the collection, use, processing, and storage of their data. Data-collecting agencies and organizations must provide information transparently and clearly. The right to rectify: Data subjects have the right to request the correction, supplementation, or amendment of their personal information if it is inaccurate or no longer necessary. The right to erasure: Data subjects have the right to request the deletion of their personal information when there is no longer a legal basis or purpose for retention. The right to access: Data subjects have the right to access their personal information to verify how the data has been processed. The right to object: Data subjects have the right to object to the processing of their data in certain specific cases, such as when the processing is based on their consent.
The right not to be subject to automated decision-making: Data subjects will not be subject to decisions about their rights, obligations, or interests based on automated processing unless they have consented or it is permitted by law. The right to complain: Data subjects have the right to lodge complaints about the processing of their data with the state management authority for information technology or other competent authorities.

The responsibilities of organizations collecting and processing personal information, also referred to as "data processors," encompass several crucial obligations as per Vietnamese law, including Lawful data collection, data processors must lawfully collect personal data, relying solely on reasons permitted by law. They are not allowed to gather personal information unlawfully or without the consent of the data subjects; By Providing information to data subjects, data processors are obligated to provide clear and transparent information to data subjects regarding the collection and processing of personal data. This includes specifying the purpose of data collection and processing, the retention period, and the rights of the data subjects; Data security appropriate security measures must be employed to ensure the safety of personal data and prevent unauthorized access or data breaches; Limiting data processing data processors is only permitted to process personal data for specific and lawful purposes. They cannot use personal information for other purposes without the consent of the data subject; Respecting data subject rights, data processors must adhere to data subjects' requests, including rights of access, modification, deletion, and objection to data processing; Reporting data security violations, data processors are required to report data security breaches to state management authorities for information technology and other competent agencies when such breaches occur; Data retention, personal data must be retained or copied in accordance with legal regulations, and it must be disposed of following the appropriate procedures when it is no longer needed; Ensuring transparency, data processors must ensure transparency in the processing of personal data and maintain relevant documents and records for future audits; Cooperation with state authorities, data processors are required to cooperate with state management authorities for information technology and comply with data protection requirements.

Moreover, Vietnamese law specifies certain situations where data processors do not require the consent of data subjects. These include Emergency Cases: When there is an urgent need to process personal data immediately to protect the life and health of the
data subject or others, and the data processor is responsible for proving that their actions comply with cases permitted by Vietnamese law. Processing by State Authorities: The processing of data by state authorities with jurisdiction is allowed in emergencies related to national defense, national security, public order, social safety, major disasters, or serious diseases. Impending Threats: In situations where there is a risk of threats to security and national defense but emergency status has not been declared. Preventing Disorder and Crime: To prevent and combat disorder, terrorism, and violations of the law by legal regulations. Contractual Obligations: For fulfilling contractual obligations between the data subject and relevant agencies, organizations, or individuals as stipulated by law (Article 17 of Decree 13).

If data processors violate these obligations, they may be held legally responsible and subject to penalties as stipulated by Vietnamese law. Violations of regulations related to storage, leasing, transmission, provision, access, collection, processing, exchange, and utilization of information may incur fines of up to 200 million Vietnamese Dong (Article 9 and Article 102 of Decree No. 15/2020/ND-CP, regulating administrative sanctions in the postal, radio frequency, information technology, and electronic transactions sector) or imprisonment ranging from 6 months to 7 years (Article 288 of the 2015 Criminal Code, as amended and supplemented in 2017). Furthermore, individuals engaged in such unlawful activities may face additional penalties such as the obligation to return any unlawfully gained profits or the revocation of their business license.

4.2 THE CHALLENGE OF PERSONAL DATA SECURITY IN VIETNAM IN THE DIGITAL AGE

Personal data security is an extremely important issue in the current digital age in Vietnam, much like in many other countries around the world. According to Forbes Magazine's assessment, Vietnam has ambitious plans to lead in AI, and Vietnam hopes to be among the top 4 countries in Asia in terms of artificial intelligence progress. FPT Software is actively promoting this goal. FPT Software is also heavily investing in AI R&D to support Vietnam in entering the top 50 in the world by 2030 in AI research and development as well as software applications. Additionally, FPT Software is the first company in Southeast Asia to join the Mila partner network, the world's largest academic research lab specializing in deep learning (Gordon, 2023).
To address the challenges in cybersecurity and personal data security in the digital age, on the afternoon of September 8th, in Hanoi, at the First National Congress, Term I (2023-2028) of the National Cybersecurity Association, several critical points were raised. The congress emphasized that in recent years, the cybersecurity landscape has become increasingly complex, amidst the rapid and robust development of scientific and technological revolutions, while domestic development lags. Fierce competition among major countries in the field of cybersecurity is intensifying, deeply affecting global political security, and posing numerous difficulties and challenges in ensuring sovereignty, security, and national interests in cyberspace (Nam, 2023).

Some common personal data breaches include: Personal data breaches in Vietnam occur through several common methods, such as:

First, malicious code or malware is any program that is harmful to computer users and comes in various forms, such as computer viruses, Trojans, malware, spyware, and so on. The method of introducing this malicious code into a computer is that attackers embed these codes within normal advertisements on news websites, classifieds, or social media platforms like Facebook and YouTube. When users click on them, they can immediately infiltrate the personal computer if there isn’t a strong enough firewall to block them, and the attacker may steal important information like bank account details, credit card numbers, Gmail, Facebook, or Zalo accounts (Subramanyam, et al., 2003).

**Figure 1**

*Malware Attack Method*

There have been numerous such attacks, such as the case where a hacker was selling customer data from Vietnamese telecommunications companies, electricity
providers, banks, and businesses on a hacker forum. This is a concerning issue with the potential risk of malicious parties exploiting the stolen data for fraudulent activities. According to a report by the Vietnamese Ministry of Public Security, there are now companies providing software services to customers for unauthorized personal information collection. This software is discreetly installed on e-commerce websites to gather personal information. When users access these websites, businesses collect more detailed information about the browsing session, such as IP addresses, timestamps, phone numbers, and locations. In principle, only telecommunications providers know, at any given time, which IP address is assigned to which mobile subscriber (3G, 4G), malicious code, and spyware software to gather personal data over computers and mobile devices in network environments. They carry out attacks and intrusions into computer systems, disrupting and compromising the confidentiality, integrity, and availability of users' computers to steal personal information and data. This method is becoming increasingly prevalent and poses a growing threat, as exemplified by incidents such as the breach of 163,666,400 Zing ID accounts from VNG; over 5 million emails and tens of thousands of payment card details like Visa, credit cards, believed to be from Thế Giới Di Động and Điện Máy Xanh; and nearly 2 million customers of Hàng Hải Bank whose information was posted online (Nam, 2020).

Secondly, there are deceptive attacks, which constitute a violation of traditional privacy rights. In these attacks, the perpetrators employ various tricks to deceive victims into disclosing crucial personal information through deceptive messages. For example, the attacker impersonates an official from a government agency and requests the victim visit a counterfeit website designed to look identical to the real organization's website, making it virtually indistinguishable. The victim then unwittingly provides all of their essential personal information, which is ultimately sent to the attacker for exploitation (Oest, et al., 2018).
Thirdly, information leakage occurs through online applications and mobile apps that require users to grant certain permissions, such as camera monitoring, contacts, access to memory, etc., to be used to collect personal information from users (Hiatt & Young B. Choi, 2016). Furthermore, the disclosure of personal information without consent is widespread. Some journalists and media outlets publish personal information about interviewees and related individuals in the public media. Most social media users do not have a sense of protecting their own and others’ personal information, carelessly sharing personal information online. Some individuals engage in unlawful activities by using others’ personal information to integrate it into negative content, violating the law for purposes of slander, defamation, or humiliation. Some sensitive personal information that should not be disclosed, such as details related to legal violations, private lives, and information about vulnerable individuals like children or those currently suffering from illnesses, is still publicly disclosed, including names and addresses.

The cybersecurity landscape in Vietnam reveals that cyber intrusions, particularly web application attacks, are prevalent. Many websites in the country do not prioritize security, making them vulnerable to intrusion and data theft. Some actors even engage in attacks on personal data storage systems and customer information, such as the internet fee systems of ISPs, to erase fees, steal information from businesses for resale to their competitors, or pilfer account passwords for fraudulent activities. According to a study by the author Xuân Long, over 14,000 phones in Vietnam were secretly equipped with eavesdropping software called Ptracker by the Vietnamese technology company Viet Hong. This software surreptitiously collected various information from the installed phones, including text messages, contacts, call recordings, phone location, video
recording, image capture, and the ability to enable or disable 3G/4G connections (Long, 2023).

Fourthly, the unlawful collection of data is a growing concern. Nowadays, many commercial service companies are collecting personal data from customers, allowing third-party partners to access personal data without strict regulations or requirements. These third-party partners then transfer, trade, or sell this data to other entities. Similarly, in a study by the author Marlene Saemann and her colleagues, it was demonstrated that the collection and control of personal data by agencies or organizations may be due to technical deficiencies or lax regulations in the provision of personal data, which can result in legal actions taken by customers (Saemann & Theis, 2022). Furthermore, individuals and businesses actively gather personal information from customers, creating personal data repositories, and analyzing and processing these types of data to conduct business and trade.

The buying and selling of personal data in the market nowadays occur in both raw and processed forms. This data is often resold multiple times and provided as a service through platforms like Databox.vn, databoxviet.com, laydata.com, laydata.net, khodata.net, databox.biz, fff.com.vn, cokhach.com, and vltoolkit.com. Raw data packages are available in various fields, including lists of personnel, internal lists (including entities like law enforcement, defense, and taxation), electricity usage, Internet subscribers, banks (including account balances), insurance, business registration records, education (parents, teachers, students), real estate (including financial capacity), selectively chosen personnel (income level, position), and lists of customers using internet services (members registered on platforms such as Facebook, FPT, vnn.com, Yahoo.com, Gmail.com, Gov.vn, Hopthu.com, Hotmail.com, and Saigonnet.vn). These data types are bought and sold over extended periods with commitments to accuracy, data updates, and the ability to export data according to the buyer's requests.

The source of this raw data likely originates from the internal systems of government agencies, state organizations, or electronic administrative systems. Upon preliminary investigation, the Ministry of Public Security of Vietnam has identified over 60 organizations and individuals involved in the illicit trading and use of personal information and data on the Internet, including technology solution providers, real estate brokers, bank employees, state agencies, and individuals with access to electronic government systems related to education, healthcare, securities, and hospitals.
Furthermore, exploiting the public’s negligence and capitalizing on their desire for financial gain, these individuals request personal information and later misappropriate it under the guise of promotional campaigns, prize draws, online purchases, and prize-winning mini-games. Due to the lack of stringent legal regulations, comprehensive sanctions for these violations, and insufficient deterrence, the prosecution of entities engaged in the unlawful business of personal data does not meet the requirements.

In summary, the protection of personal data is a concern shared by organizations and many countries worldwide, and they have been addressing this issue for a significant period. Vietnam, on the other hand, is one of the countries with a high rate of development and internet usage. Regarding personal information security, according to the monitoring and statistics by the Ministry of Public Security in Vietnam, personal data of over two-thirds of the Vietnamese population is being stored, published, shared, and collected on the internet in various forms and levels of detail. The exposure of personal data is prevalent on the internet, with users often lacking awareness of personal data protection. Data is either publicly disclosed or exposed during data transfer, storage, and exchange to support business activities or due to inadequate protective measures, resulting in data theft and public exposure. Some notable cases include the leak of over 163 million customer accounts by VNG, the exposure of more than 5 million email addresses and tens of thousands of payment card details by Thế Giới Di Động and Điện Máy Xanh, the hacking incident targeting Vietnam Airlines' server system, with 411,000 member accounts of the Bông Sen Vàng program published on the internet, and the public release of customer data from FPT Company (Thành, 2022).

4.3 SOLUTIONS TO ENSURE PERSONAL DATA INFORMATION SECURITY IN THE DIGITAL AGE

As mentioned, the explosive growth of information technology poses significant challenges to data security, with personal data security presenting a substantial challenge to human security. To enforce the protection of personal data in the digital age, some countries in general and Vietnam, in particular, require a comprehensive set of solutions.

The group of national solutions: Securing personal data is of utmost importance because if data is stolen, it can lead to significant financial losses, the risk of extortion, fraud, asset misappropriation, defamation, violations of dignity, personal integrity, and
sexual assault, resulting in both physical and psychological consequences. It directly affects the legitimate rights and interests of organizations, businesses, and every individual (Online, 2021). Therefore, first and foremost, every individual needs to effectively secure their data to prevent data theft, ensure the integrity of personal information, protect their privacy, and avoid the consequences and risks that may arise from data leakage, intrusion, or theft. Furthermore, in a study by author Radi Romansky, it is also necessary to analyze potential issues that could occur and lead to undesirable consequences for those engaging in the digital world, so that future individuals can become aware of them and take necessary preventive measures to protect their privacy and identity (Romansky, 2021). Furthermore, to protect the personal data of children and mitigate potential risks to them, parents of these children should be cautious when posting images of their offspring on electronic platforms. In line with this viewpoint, author Đặng Minh Luân and colleagues have highlighted that many parents and other relatives share pictures and information about children on social networks, accidentally disclosing their data, including full names, identifying characteristics, residence, hometown, school details, class information, health status, etc. As a consequence, according to the Department of Children’s Affairs, fraudsters research their victims by gathering these data and information. During interactions through calls or chats, these individuals demonstrate a deep understanding of the victim’s psychology, enabling them to engage in targeted fraudulent activities. The victims in this context are not only the children but also their parents (Đang Minh Luan, 2023).

Firstly, solutions regarding cybersecurity technology: Firstly, it can be said that there is no absolute foolproof solution to prevent violations of personal data privacy. Depending on the various privacy breaches, we have different protection solutions. Generally speaking, there are two primary ways to stop privacy infractions on an individual basis: increasing user knowledge and utilizing computer security measures.

In the era of the expanded Internet, computer security is not just an option but a critical necessity. According to Kamat and colleagues, computer security software plays an immensely important role as the first line of defense for users against numerous potential threats from the Internet. With the ability to detect and neutralize malicious software, computer security programs such as antivirus and anti-malware software have become valuable weapons in the fight against cybercrime (Kamat, 2018). Additionally, computer security programs also detect fraudulent websites, helping users recognize
whether the websites they are accessing contain malicious code or viruses. Moreover, effective email and website filters prevent intrusions into users' privacy. Currently, major corporations like Google and Microsoft are developing and maintaining blacklists of fraudulent websites. In line with this, author Jain and colleagues in a study suggest that this list is continuously updated with contributions from the online community (Jain & Gupta, B. B., 2021). By identifying and reporting malicious websites, users also contribute to the fight against cybercrime, ensuring safety and security in the vast world of the Internet.

Furthermore, raising awareness about cybersecurity for end-users is vital in preventing personal data breaches. End-users need to be educated about the risks associated with cybercrime and equipped with best cybersecurity practices to minimize losses significantly. These practices include using strong, unique passwords with a minimum of 12 characters, including letters, numbers, and special characters, avoiding password reuse, recommending two-factor authentication, and providing an additional layer of protection to prevent unauthorized access (Verizon, 2020). On the other hand, regularly backing up data is a practical preventive measure against data loss, whether due to technical malfunctions or theft. Additionally, always installing and updating computer security software with the latest updates to avoid exploitation through outdated security vulnerabilities is a crucial step in safeguarding against malware and viruses. Lastly, exercise caution and vigilance with emails and messages from unknown sources, and limit the sharing of personal information on social media and open websites. Remember that there is no completely foolproof solution on the internet, but combining multiple protective measures will significantly minimize risks.

In Hanoi Capital, Vietnam, during the award ceremony for the "Top 10 Outstanding Digital Technology Enterprises of 2023," the Vietnam Software and Information Technology Services Association (VINASA) organized an event to vote for and honor companies in the Vietnamese ICT industry within various sectors. This event also served as a platform for introducing these enterprises to domestic and international partners and customers. During the conference, Deputy Minister Phan Tam highlighted a series of solutions, emphasizing the need to establish a skilled workforce in the digital technology sector, with larger enterprises leading and guiding smaller ones. The success secrets and market strategies of pioneering companies offer valuable lessons and direction for technology enterprises, enabling them to confidently venture into international
markets. Venturing abroad aims to conquer the limitless international market, facilitating the growth of domestic businesses and ultimately serving the Vietnamese population more effectively (Time, 2023).

Secondly, national legal solutions: Conduct research, organize implementation, and strictly enforce regulations regarding the protection of personal data through various methods, with a particular focus on informing and instructing all employees about their rights (including the right to know, the right to consent, the right to access, the right to withdraw consent, the right to delete data, the right to restrict data processing, the right to provide data, the right to object to data processing, the right to complain, report, and use, as well as the right to claim compensation for damages) and obligations (such as protecting their data, requesting other relevant organizations and individuals to protect their data, respecting and safeguarding the personal data of others, providing accurate personal data when consent allows processing, participating in advocacy and dissemination activities on personal data protection skills). According to the author Nguyen Thi Lam, compliance with legal regulations on personal data protection and participation in preventing and addressing violations of personal data protection regulations, while clearly defining responsibilities to ensure compliance with the law's provisions and timelines (Lam, 2023).

Improving and expanding the scope of regulations related to handling violations is necessary. As analyzed earlier, the enforcement of sanctions for privacy violations in general and individual privacy data in Vietnam currently lacks the necessary rigor compared to similar standards in Europe and many other countries. According to authors Vu Cong Giao and Le Tran Nhu Tuyen, the handling of violations should accurately reflect the severity of the violations and also ensure the necessary deterrence. For this reason, the government needs to amend related laws to establish more rigorous sanctions, especially in the administrative and civil areas, for agencies, organizations, businesses, and individuals violating privacy rights (Giao & Lê Trần Như Tuyên, n.d.).

In relationships with third parties, especially in cases where a business contracts with third parties, particularly when hiring third parties to process data for their business, it is essential that contracts clearly define each party's rights, obligations, and responsibilities. In a study by author Tran Thi Thu Phuong, it is also pointed out that, as the data controller, businesses need to include an additional provision called a Data Processing Agreement (DPA). Alongside the main contract, according to GDPR, the DPA
contains instructions on how the third party can use personal information to fulfill the contract's objectives (Phương, 2022). These measures together constitute a robust legal framework for safeguarding personal data in the digital age, ensuring the privacy and security of consumers in an increasingly complex digital environment.

Thirdly, international solutions: International cooperation on personal data protection is a matter of special concern to Vietnam. Accordingly, several policies have been enacted to adapt to the technology boom of the 4.0 era. These include the establishment of international cooperation mechanisms to create conditions for the effective enforcement of laws on personal data protection; participation in legal aid for personal data protection of other countries; Organizing conferences, workshops, and scientific research, and promoting international cooperation activities in the enforcement of laws on personal data protection; and technology transfer to serve personal data protection (Luật, n.d.).

To implement policies on personal data protection in the digital age, Vietnam needs to focus on coordinated methods. This involves mechanisms for cooperation with international partners, such as the data protection authorities of other countries, to share information and experiences, especially in investigating and handling data breaches. It also includes training Vietnamese officials and experts in privacy and data protection according to international standards. Increasing awareness of privacy rights is essential to ensuring that all parties understand personal data protection's importance. Vietnam can consider establishing a specialized national agency for personal data protection and privacy rights. Collaboration with international partners to develop and implement effective data protection technologies and solutions is another avenue, which may encompass cooperation in building secure data management systems. Vietnam should also create favorable conditions for businesses to comply with personal data protection regulations. This includes building a secure IT infrastructure and supporting businesses to adhere to data protection principles. In a study, the Author and colleagues have demonstrated that the implementation of cooperation and regular exchange of information between various state authorities, local governments, legal entities to protect the rights of personal data subjects and suppress offenses in the field of personal data (Vilor Tapakova, 2023).

In line with this view, a group of authors from the Jawaharlal Darda Institute of Engineering and Technology, India, argue that governments of countries often cooperate...
unofficially by exchanging information, investigating attacks or crimes, preventing or mitigating harmful activities, providing evidence, and even arranging for the extradition of individuals to the requesting country. Nations have also put forth international agreements directly or indirectly related to cybersecurity. International agreements applicable to criminal activities are identified, encompassing situations where the alleged perpetrators have used network systems in these activities. In addition to treaties (such as the United Nations Charter and the Geneva Conventions), widely accepted customary rules may also affect cybersecurity activities. International law also provides rules related to using force in armed conflicts. This could potentially apply to cyberattacks, including requirements such as non-combatants and civilian entities like hospitals not being intentionally targeted and the use of force being restricted to necessary and proportionate measures (Tonge, 2013).

The international cooperation process for protecting personal data needs to consider factors related to national sovereignty, privacy rights, and the self-determination of each country. International cooperation helps create a safe and secure environment for individuals’ data and ensures that Vietnam complies with international standards.

5 CONCLUSION

In the current digital age, personal data security policies play a crucial role in protecting the privacy and safety of every internet user. Alongside the rapid development of technology and the internet, the risk of personal information insecurity is also on the rise. Establishing and implementing personal data security policies is a critical step to ensure that everyone's personal information is adequately protected. Creating security policies should be based on an understanding and compliance with legal regulations regarding personal data protection. Furthermore, promoting awareness and skills related to personal data protection is essential for internet users to actively participate in safeguarding their personal information.

In the context of the expanding digital revolution, personal data security policies will continue to evolve and adapt to new challenges. The question at hand is the need to maintain vigilance and readiness to ensure that personal data is consistently protected, safeguarding everyone's privacy. In the future, promoting respect for and protection of personal data will be increasingly important in building a secure and trustworthy digital
environment. Collaborative efforts among relevant stakeholders will be crucial in advancing the goal of ensuring that technological progress goes hand in hand with the protection of personal information and privacy, contributing to the overall security of individuals in the digital age.
REFERENCES


Available at: https://datareportal.com/reports/digital-2023-vietnam

Available at: https://www.echr.coe.int/documents/d/echr/Convention_ENG

Available at: https://gdpr.eu/article-4-definitions/

GDPR.EU, n.d. What is considered personal data under the EU GDPR? [Online]
Available at: https://gdpr.eu/eu-gdpr-personal-data/


Available at: https://www.forbes.com/sites/cindygordon/2023/02/22/vietnams-ai-leadership-status-is-blossoming/?sh=47ecd1201a4e


Lam, N. t., 2023. Các giải pháp tăng cường bảo vệ dữ liệu cá nhân. [Online]
Available at: https://www.mof.gov.vn/webcenter/portal/thtk/pages_r/l/chi-tiet-tin-tinhoc-va-thong-ke?dDocName=MOFUCM286194
Available at: https://tuoitre.vn/vu-dien-thoai-bi-nghe-len-phan-lon-thue-nghe-len-doi-tu-615598.htm


Nam, B. C. A. V., 2019. Thực trạng công tác bảo vệ dữ liệu cá nhân , Hà Nội: s.n.

Available at: https://xaydungchinh sach.chinhphu.vn/thuong-tu-thuong-luong-tam-quang-duoc-bau-giu-chuc-chu-tich-hiep-hoi-an-ninh-mang-quoc-gia-119230908182809514.htm

Available at: https://baophapluat.vn/bo-cong-an-danh-gia-nan-danh-cap-mua-ban-du-lieu-ca-nhan-rat-phuc-tap-post330874.html


Online, Đ. T., 2021. Tầm quan trọng của bảo mật dữ liệu cá nhân trong thời đại số. [Online]

Phương, T. T. T., 2022. Quy định chung của Liên minh châu Âu về bảo vệ dữ liệu cá nhân và một số khuyến nghị đến Quốc hội, Chính phủ và doanh nghiệp Việt Nam. [Online]
Available at: http://lapphap.vn/Pages/tintuc/tinchitiet.aspx?tintucid=210980

Available at: https://edps.europa.eu/about-edps/supervisors_en

Available at: https://www.echr.coe.int/european-convention-on-human-rights

Available at: https://www.jstor.org/stable/20027310


Available at: https://quochoi.vn/pages/tim-kiem.aspx?ItemID=67343

Time, V., 2023. Thủ trưởng Phan Tâm: 3 việc cần làm của ngành TT&TT và các DN công nghệ số. [Online]
Available at: https://viettimes.vn/thu-truong-phan-tam-3-viec-can-lam-cua-nganh-qttt-va-cac-dn-cong-nghe-so-post170192.html


Available at: https://www.verizon.com/business/resources/security/ten-best-practices-for-internet-security/