**Journal of Information Systems Engineering and Management**
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

# Protecting Privacy when using Artificial Intelligence in Retail systems: Legal regulations in the US, EU and Vietnam

Phan Dang Hai[1], Nguyen Thai Ha[2], Nguyen Thi Mai Dung[3], Nguyen Thi Hue[4]
[1] *Banking Academy of Vietnam, Vietnam. Email: haipd@hvnh.edu.vn*
[2] *Banking Academy of Vietnam, Vietnam. Email: hant@hvnh.edu.vn*
[3] *Banking Academy of Vietnam, Vietnam. Email: dungntm@hvnh.edu.vn*
[4] *Banking Academy of Vietnam, Vietnam. Email: huent.bn@hvnh.edu.vn*

**ARTICLE INFO**

Received: 30 Dec 2024

Revised: 19 Feb 2025

Accepted: 27 Feb 2025

**ABSTRACT**

The rapid development of technical technologies used by offline and online retailers has made consumers' concerns regarding privacy increasingly heightened. With that comes countless tensions for retailers and consumers, trade-offs and compromises just to personalize the shopping experience. In this article, we study privacy regulations when businesses use artificial intelligence in retail systems in the United States - a leading country in artificial intelligence, the European Union - the European Union. The region has the strictest privacy legal policies and Vietnam - a developing country with great potential in artificial intelligence. Based on the mentioned legal regulations, we provide an overview of the data privacy risks that artificial intelligence can bring in the retail industry and the reasonable ways in which Governments of developing countries should react so as not to unintentionally inhibit the development of the digital economy by their strict legal policies. Along with that, our research direction also lays a promising foundation for academic research on privacy rights and a model for building privacy protection laws that take into account the balance between the law and the law. and economic development orientation.

**Keywords:** Data privacy; Retail industry; Artificial Intelligence; Legal model of privacy.

## 1. INTRODUCTION

Artificial intelligence (AI) is a product of modern technology that allows simulation of human intelligence. AI can replace humans to perform important tasks with high efficiency. The Global AI Adoption Index shows that the global AI technology application rate in 2022 has reached 35% [18]. AI is increasingly widely applied and has the potential to play a central role in the retail system in the new era. Among them, Amazon, Walmart, and Target are leading corporations in applying AI to retail activities. AI is a powerful tool that helps retailers analyze large amounts of data, forecast demand, optimize pricing strategies, improve cost efficiency , and boost business revenue and profits.

However, in addition to revolutionary and groundbreaking utilities in human activities in general and in retail services in particular, AI can also perform acts that violate human rights. In particular, customer privacy is one of the prominent issues discussed as the trend of using AI to support retail activities at businesses is increasing. AI technology is becoming more advanced, allowing the collection and analysis of a huge amount of data about individuals including their behavior, preferences, and even thoughts and emotions in order to Train the algorithm and improve performance in making predictions about customer profiles, improving the efficiency of business product marketing. The main concern surrounding AI collecting personal customer information is what that information will be used for and who has access to that information system. Customer data information such as purchase history, demographics, and biometrics that AI collects can be abused to create fake profiles or manipulate images for many other purposes. each other.

Integrating AI technology in business operations has become popular in retail businesses in Vietnam today (including both domestic and foreign-invested businesses). AI technology is applied in many situations such as supply chain planning, market demand forecasting, inventory management, and personalizing customer experience. Therefore,

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

promoting the development and strong application of AI in the retail industry is one of the key views of the Vietnamese government expressed in the National Strategy on research, development and application of Artificial Intelligence. created until 2030 [15]. Besides, in 2022 Vietnam is ranked 55th out of more than 180 countries and territories on the government's artificial intelligence readiness index [39]. However, the legal system protecting privacy when applying artificial intelligence to the retail system in Vietnam is still not highly appreciated. Vietnam has not yet issued any separate legal documents on privacy protection when using AI in the retail industry. Current regulations related to this field are only scattered in general legal documents and some specialized legal documents such as the 2015 Civil Code (Article 38), Penal Code 2015, amended and supplemented in 2017 (Article 37), Decree No. 13/2023/ND-CP on personal data protection... In general, the above legal regulations only focus on rules related to the right to know the purpose of collection, scope of use, and storage period of personal information; consent and authorization to process individual data without any specific regulations on the processing and use of big data... There are also many specialized seminars related to privacy protection in the era of However, in-depth studies on privacy protection when using artificial intelligence in retail systems focusing on legal issues in the current Vietnamese context are very rare. Therefore, the purpose of this study is to provide suggestions that contribute to improving legal policies when using AI in retail that governments of developing countries can refer to in order to strike a balance between promulgating laws and developing technology in the digital age. To achieve that result, we researched the legal status of privacy protection in the retail sector in the United States - representing the leading country in artificial intelligence development; EU - the region with strict privacy policies in the world and Vietnam . This research also points to the fierce conflicts between consumers and retailers that appear throughout the sales cycle, trade-offs and compromises towards personalization of the shopping experience.

## 2. METHODOLOGY

The research method used in the article is mainly desk research. The authors mainly analyze and synthesize information, figures, and data collected from annual reports of ministries and ministerial-level agencies in Vietnam, articles in prestigious scientific journals, domestic and foreign electronic information sites. A comprehensive review of the development of Vietnamese legal regulations protecting individual privacy when using AI in retail systems was conducted. On the basis of current legal regulations, the authors use analysis and evaluation methods to see an appropriate legal development model to regulate privacy rights for Vietnam in particular and other countries with growing economy in general .

In addition, the authors also conducted research on legal regulations on protecting the privacy of individual customers in Vietnam from a comparative perspective with legal regulations in the European Union, the EU and the United States. Legal documents on privacy in Vietnam, the EU, and the United States are collected from official sources of the governments of the countries, and are included in an evaluation table for comparison purposes to see differences. differences and shortcomings of legal regulations. Based on the differences that have been researched, the authors discuss and explain the differences, thereby drawing lessons from the experiences of Vietnam and other countries with different economic situations and development orientations. Similarities can be referenced. In addition, the presented research results may also open new directions for future academic research on privacy in retail. Below, the authors describe the research and document analysis process used in this study (Figure 1).

## 3. RESEARCH RESULTS

### 3.1. Application of AI in the retail system and judicial practice of privacy invasion through artificial intelligence in the retail system in Vietnam

The deep origins of Artificial Intelligence can be traced back centuries ago when philosophers tried to explain the human mind as a symbolic system. However, modern AI really began to take shape in the mid-twentieth century when American computer scientist John McCarthy first proposed the concept of *"Artificial Intelligence"* at the Dartmouth Conference in 1956 [23]. Since that time, artificial intelligence has continuously developed and has become an indispensable part of modern life, present in most industries and fields in the forms of: machine learning, machine vision. computing, natural language processing, voice recognition. by 2027 (407 billion USD), which is a significant growth from the estimated revenue of 86.9 billion USD in 2022 [9]. In the retail industry, AI also proves its importance in customer relationship management, inventory management, content production, supply chain

**Journal of Information Systems Engineering and Management**
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

operations... In recently published statistics, Forbes Advisor surveyed 600 business owners who are using or planning to incorporate AI in business, the percentage of businesses using AI to perform the above activities is 46%, 40%, 35% and 35% respectively 30% [10].

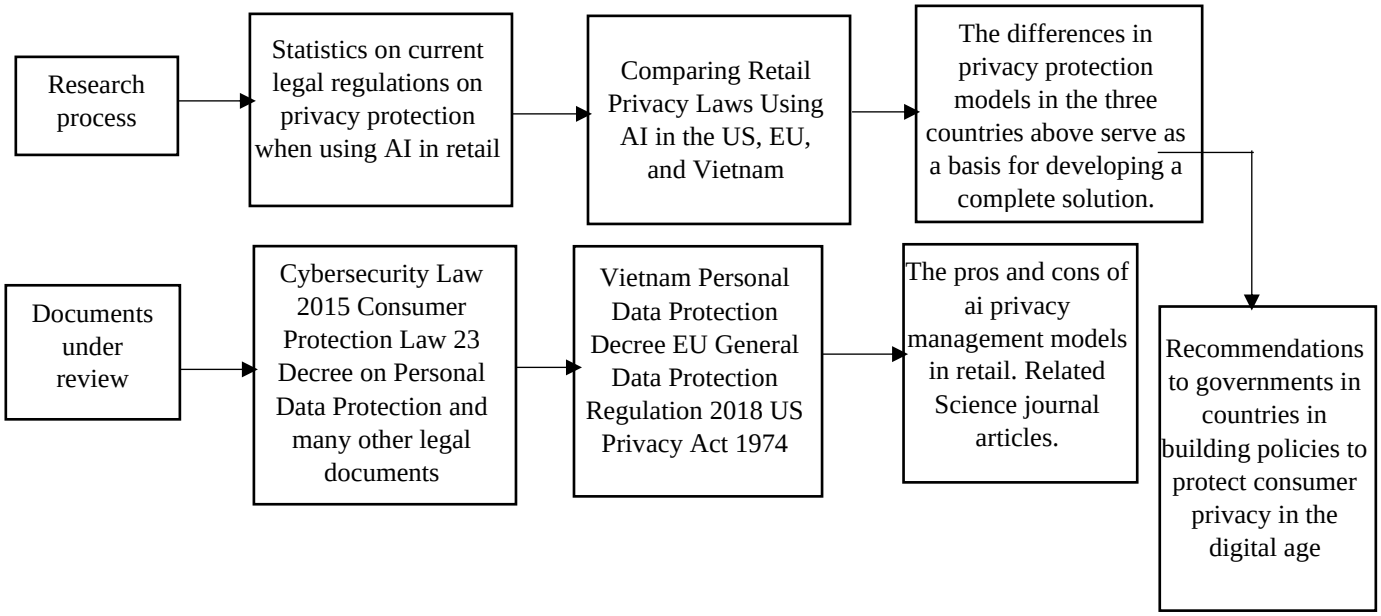


**Figure 1.** Document research process used in the article

Today, with many diverse applications, artificial intelligence is considered a valuable resource that helps businesses improve operational efficiency, save time and reduce costs. According to Forbes Advisor statistics, the AI market size is predicted to reach a staggering level Amazon, Walmart, Target are leading corporations in applying AI to retail operations. AI is a powerful tool that helps retailers analyze large amounts of data, forecast demand, optimize pricing strategies, improve cost efficiency, and boost business revenue and profits.

In recent years, Vietnam has made great strides in the fields of digital transformation and artificial intelligence (AI). According to the announcement of the Ministry of Industry and Trade, Vietnam's retail industry currently has a market size of 142 billion USD, forecast to increase to 350 billion USD by 2025, contributing 59% of the total GDP domestic budget. The AI market in Vietnam is predicted by Statista to achieve an annual growth rate of 19.51% in the period 2023 - 2030, reaching a value of more than 1.8 billion USD [25].

Although it is in the early stage, Vietnam's potential for AI development is extremely large . Although it is a latecomer country, artificial intelligence is not as widely used as in long-standing developed countries such as the US, Canada, China... but Vietnamese businesses are now aware of its importance. of artificial intelligence and its great impacts on our production and business activities, so we constantly learn, absorb experience and are not afraid to innovate our business activities. Some leading businesses using artificial intelligence in the retail sector in Vietnam include FPT, Viettel AI, VNPT AI, VIN AI... Among them, VIN AI is the only business in Vietnam to enter the list. Top 20 leading global companies in AI research organized by Thundermark Capital in 2022, on par with many large businesses in the retail industry such as Amazon (USA), Alibaba (China).

In Vietnam, the monitoring and protection of personal information is carried out by the Department of Personal Information Security under the Ministry of Information and Communications (performing the function of advising and assisting the Minister in state management and organization) law enforcement agency on network information security [13]; Ministry of Public Security in detecting and criminally handling personal data infringement cases [14]. In addition, a number of social organizations in the field of cyber security were established such as the National Cyber Security Association under the Ministry of Public Security with members being businesses and individuals operating in the field. technology with main activities related to updating information, researching legal policies and making recommendations on the cyber attack situation in Vietnam. The National Cyber Information Security Monitoring Center (a unit under the Department of Information Security - Ministry of Information and Communications) has

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

deployed the 2022 Campaign to clean malicious code in cyberspace; The Green Shield campaign is aimed at all individuals and businesses to prevent cyber attacks and clean up cyberspace. Special, The agency's website also encourages users to send warnings about safety and network security issues and provides a number of tools for individual users to check to detect fraud and check for malicious code in their devices. network, check for fraudulent websites , check for personal account information leaks... As a result, 3,478 fraudulent websites that violate the law in Vietnam will be handled in 2023; 2.1 billion views of videos recreating and warning about online fraud on social media channels; 3.7 million people are protected from accessing online scam websites or violating laws in cyberspace [26].

Regarding judicial practice, over the past many years, the issue of personal data leaks in Vietnam is no longer strange in many fields such as telecommunications, finance - banking, e-commerce... The situation of attacks, Stealing, buying and selling personal data for profit is common on the Internet and social networks; Groups of subjects who illegally purchase and sell personal information are often people with a deep understanding of information technology; taking advantage of cyberspace to commit crimes using high technology and sophisticated tricks. That is why currently, personal data of 2/3 of Vietnam's population is being stored, posted, shared and collected in cyberspace in many different forms and levels. Data files are clearly classified by job, hobbies, location, marital status, children, income... and divided into data packages for many different customer segments to serve buyers. data in advertising, offering products or more dangerously, fraud, appropriating bank accounts, or stealing money. Typically, personal data is offered for sale by target groups right on websites that people can easily search with just one mouse click after typing on the Google search toolbar about personal data. According to the summary report of the Ministry of Information and Communications in 2022, revenue in the field of network information security alone reached VND 4,835.4 billion, an increase of 26.15% compared to 2021, but the number of losses in in the same field is very large, about 21,200 billion VND, the average cost to fix leaks, data leaks or stolen data is up to 15.4 million USD/case [26]. This has caused causing data, economic, brand damage, business interruption and costly troubleshooting time.

In the retail sector in Vietnam, many cases of serious infringement of customer privacy rights have also been recorded. Through a preliminary review, the Ministry of Public Security discovered more than 60 organizations and individuals involved in illegal trading and use of information and personal data in cyberspace in two main forms: (i) Enterprises with service business activities that collect personal data from customers, allowing third parties to have access to personal data information but without agreements or legal bindings for third partners three transfer and trade to other partners; (ii) businesses proactively collect customers' personal information to form a personal data warehouse, then analyze and process that type of data to serve their business activities. Retail stores or some online shopping websites require customers to provide personal information when making purchases. In April 2018, the data of 163,666,400 Zing ID accounts of VNG Joint Stock Company was offered for sale on a site specializing in international data sharing and trading. In November 2018, more than 5 million emails and tens of thousands of payment card information such as Visa, credit cards, were believed to belong to Mobile World Company Limited and Dien May Xanh Investment - Development Company Limited. Mobile World and Dien May Xanh are two large retailers in the electronics industry in Vietnam with market shares of 24.2% and 46.9%, respectively [28]. In November 2019, nearly 2 million customer data of Vietnam Maritime Commercial Joint Stock Bank including information about full name, ID card number, occupation, email, phone number, residential address, date of birth, gender was posted online [29].

As a leading country in the development and use of artificial intelligence in general and in the retail industry in particular, in the United States, the average cost of a data breach is up to 9.48 million USD [1]. Notable data breaches when businesses use artificial intelligence in their business operations include: In December 2023, Rite Aid Group with the Rite Aid pharmacy chain was banned by the Commission. The US Federal Trade Commission (FTC) issued a five-year ban on the use of facial recognition technology for surveillance purposes due to the system’s flaws in misidentifying consumers, especially women. Women, children and people of color are shoplifters, causing a negative impact on customers’ reputation [8]. In May 2013, Amazon - a large retail corporation could not avoid accusations from the US Federal Trade Commission and the US Department of Justice that this business had collected huge amounts of data about customers. their consumers through the Alexa app, preventing parents from exercising their right to deletion under the COPPA Rule, retaining children's geolocation and voice data for years and using it for

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Model training section to understand children; thus seriously infringing on children's online privacy. According to the FTC's announcement, in addition to the data deletion requirement in the proposed order, Amazon will have to pay a civil penalty of $25 million and implement a number of other provisions of the proposed order [32].

### 3.2. Vietnam's legal system on protecting privacy when using AI in the retail system

Currently, Vietnam has not yet issued any specific law related to protecting privacy and protecting personal data. Legal regulations on protecting individuals' privacy when using AI in retail systems are still in their infancy, mainly adjusted based on scattered legal regulations on privacy protection. in Codes, laws and decrees. The current legal system in Vietnam on AI in retail is stipulated in the Constitution and 05 Codes of Law; 02 Government Decree, although not yet completely completed, has become an important legal basis, providing basic legal protection measures for citizens' personal information.

**Table 2.** Current Vietnamese legal regulations on protecting personal privacy in the retail sector

| Type of legal document | Name of legal document | Effective date | Related terms |
|---|---|---|---|
| Constitution | 2013 Constitution | 01 January, 2014 | Article 21 |
| Code | Civil Code 2015 | 01 January, 2017 | Article 38 |
| | Penal Code 2015, amended 2017 | 01 January, 2018 | Article 159 |
| Law | Cyber security law 2018 | 01 January, 2019 | Chapter III; Chapter IV; Chapter V |
| | Commercial Law 2005 | 01 January, 2006 | Clause 4 Article 78 |
| | Law on network information security 2015 | 01 July, 2016 | Article 17 |
| | Law on protecting consumer rights in 2023 | 01 July, 2024 | Clause 1, Article 4; Point Clause 1 Article 10; Article 15; Article 16; Article 17; Article 18; Article 19 |
| | Electronic transaction law 2023 | 01 July, 2024 | The law sets out regulations when conducting transactions by electronic means |
| Decree | Decree No. 13/2023/ND-CP on Personal Data Protection | July 1, 2023 | The Decree provides legal regulations on personal data protection activities and responsibilities of competent state agencies in protecting personal data. |
| | Decree No. 15/2020/ND-CP regulating penalties for administrative violations in the fields of postal, telecommunications, radio frequency, information technology, network information security and electronic transactions | January 27, 2022 | Section 2 Chapter V |

*(Source: Legal documents)*

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

### 3.3. Compare regulations on using AI in retail systems of Vietnam, US, and the EU

Currently, there are four main international legislative models used to protect privacy: the global model, the co-regulation model, the sector model and the self-regulation model [22]. In fact, the models listed above also have certain similarities such as adhering to the principles of balanced information, providing legal measures for individuals to ensure their rights, determining personal data processing parameters, requiring organizations to post notices clearly stating the categories of personal information collected. On the other hand, if the EU protects consumers' personal information along with personal information, other personal information in a fully integrated manner, applying regulations such as the EU Data Protection Directive 1995 (95/46/EC) and the General Data Protection Regulation 2018 (GDPR); The United States has built its retail privacy legal system on an industry model, that is, different regulatory agencies are responsible for implementing and enforcing regulations in their respective sectors, e.g. such as the Consumer Financial Protection Bureau or the U.S. Department of Health and Human Services [22]. Vietnam, with its scattered retail privacy protection regulations, has been making efforts to comprehensively protect personal information. In the retail industry's management of consumer information, differences are seen between Vietnam, the United States and the EU (Table 3).

**Table 3.** Differences between Vietnam, the US, and the EU in managing personal information in the retail sector

| Content | Vietnam | European Union (EU) | USA |
|---|---|---|---|
| Concept | *Personal data* includes basic personal data and sensitive personal data (Clause 1, Article 2, Decree No. 13/2023/ND-CP).<br>*Sensitive personal data* is personal data associated with an individual's privacy rights that, when violated, will directly affect the individual's legitimate rights and interests (Clause 4, Article 2, Decree No. 13 /2023/ND-CP) | *Personal data* is any information relating to an identified or identifiable natural person by reference to an identifier such as a name, location data, online identifier or one or more specific physical, physiological, genetic, mental, economic, cultural or social factors of that natural person (GDPR Article 4) | Sensitive personal data includes personal health data, financial data, creditworthiness data, student data, biometric data, personal information collected online from children are under 13 years of age and the information could be used to commit identity theft or fraud. |
| Consensus | Personal data may only be used with the individual's consent.<br>(Clause 2, Article 11, Decree No. 13/2023/ND-CP)<br>The data subject's consent must be expressed clearly and specifically in writing and voice (Clause 3, Article 11, Decree No. 13/2023/ND-CP) | Consent may be in writing (including electronic) or in the form of an oral declaration (GDPR, Article 7).<br>The consent request must be presented in a clear and understandable manner | Individual authorization of your data must be in writing. (45 CFR § 164.508) |
| Exceptions to consensus | Unless legal documents provide otherwise (Clause 1, Article 11 of Decree No. 13/2023/ND-CP) | There is no exception to the consent of the data subject when entering the retail system (EU General Data Privacy Regulation, GDPR, Article 9) | Provides exceptions to the authorization requirement for (1) individuals (unless access or disclosure of accounting information is required); (2) treatment, payment and health care operations; (3) opportunity to |

**Journal of Information Systems Engineering and Management**
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

| | | | |
|---|---|---|---|
| | | | agree or object; (4) other permitted disclosures and uses; (5) public welfare and benefit activities; and (6) limited data sets used in research, public health, or health care operations e. (45 CFR § 164.502(a) |
| Withdraw consent | Withdrawal of consent does not affect the lawfulness of the processing of data agreed to before the withdrawal of consent.<br>The withdrawal of consent must be expressed in a format that can be printed, copied in writing, including in electronic form or verifiable format (Article 12 of Decree No. 13/2023/ND- CP). | Data subjects have the right to withdraw their consent at any time. Withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal. Withdrawing consent will be as easy as giving consent (EU General Data Privacy Regulation, GDPR, Article 7) | In general, individuals have the right to withdraw consent at any time, as long as the revocation is in writing. (45 CFR § 164.508(b) |
| Right to erasure and right to be forgotten | Data subjects are requested to delete their personal data in the following cases: a) Realizing that it is no longer necessary for the purpose of collection, and has agreed and accepted possible damages when requesting deletion data; b) Withdraw consent; c) Object to the processing of data and the Controller of personal data, the Controller and processor of personal data do not have a legitimate reason to continue processing; d) Personal data is not processed for the agreed purpose or the processing of personal data is in violation of the law ; d) Personal data must be deleted according to the provisions of law (Article 16 of Decree No. 13/2023/ND-CP) | The data owner has the right to request the deletion of personal data relating to him or her in the following cases: (i) The personal data are no longer necessary in relation to the purpose for which they were collected; (ii) the data owner requests deletion; (iii) the data owner objects to the data processing; (iv) data processed unlawfully; (v) personal data must be erased for compliance with a legal obligation under EU or member state law; (vi) personal data collected in connection with the provision of information society services (EU General Data Privacy Regulation, GDPR, Article 17) | Must maintain privacy policies and procedures, notices of privacy practices, complaint handling, and other actions, activities, and designations that the Privacy Rule requires to be recorded must be retained at least six years after its creation or final effective date (45 CFR § 164.530(j)) |

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

| | | | |
|---|---|---|---|
| Data management system | Enterprises providing services in cyberspace are responsible for applying necessary measures to ensure security for the information collection process, preventing the risk of exposure, leakage, damage or loss of human information data. use (Point c Clause 1 Article 41 Law on Cyber Security 2018) | A data protection officer will be appointed if the core activities of the data controller or processor include the processing of special categories of personal data on a large scale (including data relating to health and safety). health of natural persons) (According to the EU General Data Protection Regulation, GDPR, Article 37) | Covered entities must designate a privacy officer responsible for developing and implementing their privacy policy. Additionally, covered entities must designate a contact person or liaison office responsible for receiving complaints and providing information to them (45 CFR 164.530(a)). |

*(Source: Legal documents)*

## 4. DISCUSSION

### 4.1. The difference between the concept of personal information and the concept of personal privacy

Personal information and privacy are two intimate concepts that, although closely related, have important differences. Defining the concept and scope of privacy is important in resolving current legal disputes. Especially in the context of the development of international trade in digital services, the boundaries of privacy protection have become vague, expectations of data privacy protection have been seriously reduced, and most of all, the public tends to normalize the sharing of personal information [46] From a legal perspective, personal information refers to any information about a specific person or that can identify a specific person, such as name, address, phone number, or image, some The country has been considering information privacy and personal data as a human right, on par with other basic rights. Meanwhile, there is no unified definition of the right to privacy. A Hungarian scholar has argued about the right to privacy: Privacy is the right of the individual to decide about himself.

The intertwining of personal information and privacy, along with economic development perspectives and the construction of different legal systems, has created legal protection models for personal privacy and personal information. different individuals in some countries and territories. In our research, we discovered two distinct privacy protection models between the US and the EU. The United States applies a consistent model of privacy protection and personal information protection through privacy protection provisions. Meanwhile, EU law tends to gradually separate personal data protection from privacy protection and considers personal data protection as one of the basic human rights [2]. The 2018 EU GDPR regulation mentioned “the right to the protection of personal data” (Article 1), highlighting the independent nature of personal data protection [12]. The reason for this difference is because the United States uses a sectoral approach to privacy, based on a combination of law, economic policies, and self-regulation; Besides, comprehensive frameworks governing privacy in general and data privacy in particular have not been built like the EU [2]. In general, the two studied privacy management models both bring certain advantages but also contain many disadvantages. With a management model like the EU's, the government will not spend many resources to handle risks, but this overly broad approach will also inevitably stifle technological innovation. As for the US approach, which is very encouraging for technology to develop but is easily abused, tightening information control requires close coordination between agencies to build common management tools.

In Vietnam, privacy protection and personal information (personal data) protection are regulated according to a unified model of privacy protection. Provisions on privacy protection are mentioned in the 2013 Constitution (Article 21) and the 2015 Civil Code (Article 38). In particular, Decree No. 13/2023/ND-CP on personal data protection has established a standard for classifying personal data. Accordingly, personal data includes sensitive personal data and basic personal data (Clause 1, Article 2). Sensitive personal data is personal data associated with an individual's privacy that, when violated, will directly affect the individual's legitimate rights and interests (Clause 4, Article 2). Sensitive personal data includes data on political and religious opinions; health status; racial origin; genetic

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

characteristics; physical attributes and biological characteristics; sexual life and orientation; criminal records; credit accounts; personal location determined through location services and other data that the law deems necessary to be protected (Article 2, Clause 4). This model is said to be quite similar to the model of privacy and personal data protection prescribed in China - a country with a political system quite similar to Vietnam [6].

### 4.2. Data collection issues and challenges when data is collected across borders

#### *4.2.1. The problem of data collection using artificial intelligence in the retail industry*

In the retail sector, to personalize customer needs towards the goal of revenue and profit growth, sellers always find ways for customers to share information, location, preferences, and needs. them freely. Many academic studies on privacy in retail also show that user data privacy can occur throughout the process of consumers participating in purchase transactions on websites and media channels. social networks, on mobile phones or at direct retail stores [20], especially in the context of businesses trying to apply artificial intelligence technology to their business activities.

Before purchasing. This phase includes the time from pre-purchase to actual purchase [21]. Although not given much attention, data breaches often occur during this phase. Specifically, salespeople can secretly follow search history, collect and analyze information about customers' voices, social network posts, and customer call messages to identify customers. See which products should be recommended during a customer's search to increase the likelihood of a purchase. In some cases, customer data is also used for the purpose of creating asymmetric transactions. For example, businesses collect financial data about customers and then sell products and goods to them at higher prices than normal.

Purchase. In fact, the moment of purchase is the time when retailers often collect consumer information and is also the time when consumers are willing to share their information. Retailers may ask consumers to fill out information forms if the transaction is made on digital channels or customers will have to provide information related to name, age, contact information, geographic location, etc. as requested by sales staff in a traditional environment. In addition, if making transactions at traditional stores, consumers are also at risk of having their facial recognition data, biometric data, shopping habits, preferences, etc. collected by artificial intelligence through cameras installed in the store.

After purchase. The post-purchase stage is the stage that strengthens customers' desire to buy in the future and even builds a loyal customer group, so many businesses are very interested in customer experience. They collect customer data by monitoring reviews, monitoring customer posts on social networks or more dangerously, using smart devices using modern technology (robot vacuum cleaners, taxis). unmanned vehicle...) will automatically monitor and collect data about consumer behavior to send to the server system. At this stage, the privacy invasion is less noticed by users, creating conditions for retailers to repeat the above process.

Studying the process of businesses collecting user data, the authors found a serious conflict between the desires of consumers and businesses. On one hand, consumers want businesses to personalize their shopping experience to save time and effort in finding suitable products and services; On the other hand, a part of consumers does not want to provide too much personal information and expresses concern when personal data is used for the wrong purpose. One study found that more than 70% of consumers expressed disappointment when their shopping experience was not personalized [41], and 70% of consumers surveyed said they felt concerned when shopping. Businesses use the data they provide [3] Currently, the personal data processing rules analyzed in section 4 include prior notification, obtaining individual consent, and not excessively collecting sensitive personal data except in the following cases: special cases permitted by law. Many digital applications in general and e-commerce applications in particular have assigned their consumers agreements regarding the use of their personal data. These agreements are part of their privacy policies that are publicly posted on the Internet, however, these policies are difficult for the average user to understand and sometimes users choose not to pay attention to their rights. For your privacy, accept consent to use the application, because not using Google, Amazon, not participating in Facebook means not participating in the information society for many people. Many privacy studies show that privacy policies are difficult to read and vague. It can take the average person up to 250 hours of work per year just to actually read the privacy policies of the websites

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

they actually visit over the course of a year [42]. So, the question is how can consumers personalize their shopping experience without violating their privacy?

#### *4.2.2. Challenges when data is collected across borders*

The relationship between cybersecurity and data restrictions is a relatively underexplored area of research despite being a growing concern in international trade. The free flow of data is one of the important factors for developing Artificial Intelligence. However, the widespread application of AI models and cross-border data flows can conflict with privacy policies. Looking at it another way, it is possible that strict legal policies on privacy also invisibly limit the development of artificial intelligence in particular and the technology industry in general. Despite the benefits of free data, countries around the world still impose some restrictive policies to address data privacy concerns.

The European Union The EU has developed a data privacy policy early on that includes provisions restricting the transfer of data outside the European Economic Area and to countries that do not adequately ensure data system security (Chapter V GDPR). On the other hand, the United States chooses a model to manage the flow of data sources more freely than the EU, but that does not mean that data privacy in this country is weakened. Although not specifically stipulated in major legal documents, restrictions on cross-border information transfers are bound by the United States in its regional trade agreements (such as the USMCA and the US-Japan Digital Trade Agreement) [38].

In recent years, Vietnam has been considered one of the 10 countries with the largest amount of cross-border data flow in the world [19]. This positively reflects Vietnam's potential and opportunities, and at the same time, comes with a huge challenge in the process of protecting user data without damaging the data flow. Meanwhile, legal regulations in Vietnam in this field are still at a primitive level. The Decree on personal data protection that will take effect in July 2024 also has regulations on cross-border transfer of personal data, but it is not really clear, regulations on conditions for transferring personal data. across the border, there is an overlap between the transfer conditions and the transfer exception, between the transfer exception and the condition that the Personal Data Protection Commission issues a written consent to the transfer. In the field of international trade, Vietnam has participated in many free trade agreements, but most of these agreements do not include provisions on cross-border data flow. It is agreed that different countries have different information security standards as well as apply different legal models regarding cross-border data flows. Therefore, when building a reasonable management model for cross-border data flows, each country needs to consider both economic and privacy concerns, and must balance technological and economic development. with privacy protections.

#### *4.2.3. The balance between economic development in the digital age and privacy protection measures*

In a classic study on the right to privacy by Warren and Brandeis (published in the Harvard Law Review in 1890), scientists recognized technological development as one of the phenomena that poses a threat to human rights. human privacy [45]. Therefore, in the face of economic, political and social changes, the law must always develop and create new rights to “meet social needs” and ensure full protection for people and their families asset [11]. Looking at it another way, data-driven innovation and digital commerce will become increasingly important to the global economy. It is absolutely necessary for governments to update legal policies to address legitimate privacy concerns, but policies need to be enacted and implemented in a way that makes sense to citizens, businesses and the Government can maximize huge economic and social benefits from huge data sources and advanced technologies. Unreasonably strict privacy requirements in data processing should be avoided as this could indirectly hinder the development of privacy. When developing legal policies on consumer privacy, it is imperative to consider the economic interests of retail businesses.

In this section, the authors give some recommendations to develop a policy to protect consumer privacy in the face of the strong rise of artificial intelligence in a reasonable way, including a balance between economics, law and society.

Recommendations for retail businesses:

Today, businesses can fully take advantage of their privacy protection policy as a tool to attract customers. Instead of arbitrarily collecting and analyzing customer data, businesses should be customer-centric and consider building strong measures to protect consumer data. Evidence is that businesses with clear information security policies will

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

enjoy tangible benefits such as shorter sales times, reduced risks and costs due to data breaches, increased flexibility, build customer trust and loyalty [11]. Cisco's recent data privacy benchmark study found that data privacy is a very attractive financial investment for businesses. organization. On average, an organization receives a privacy benefit of 1.6 times their investment; More than 30% of organizations estimate their returns to be at least twofold, and about 12% of organizations think they are seeing returns of up to three times their investment [5].

Recommendations for governments in developing policies to protect consumer privacy:

Governments of countries with developing economies similar to Vietnam, if they want to take advantage of the advantages gained from artificial intelligence while still fully ensuring basic human rights, can research and build a legal model on privacy protection that combines the EU and US models. On the one hand, countries should build a legal system to systematically protect consumer privacy, with a combination of strict regulations and sanctions that serve as a deterrent , and mechanisms to protect consumers' privacy. Accountability also needs to be rigorously developed to ensure that acts of using AI to violate privacy rights are managed and remedied promptly. On the other hand, governments should also develop national strategies and issue many preferential and encouraging policies to promote the development of artificial intelligence in the digital age.

Vietnam and other countries with similar economies and the same development direction also need to increase participation in the development of international networks on data management in the retail sector. As a member country of the Asia-Pacific Economic Cooperation (APEC), Vietnam should also take advantage of APEC's relatively complete privacy framework as a reference document. important reference in promulgating new policies. Building on APEC's cross-border privacy rules, countries can work together to forge a common governance agreement that establishes a global data security framework.

To avoid negative impacts from citizen data being transferred across borders, some countries with developing economies like Vietnam need to consider researching solutions to minimize dependence on private parts. Foreign-developed open source software by strengthening cooperation between the government and domestic technology enterprises; Issue preferential legal policies on taxes, land and other incentives to create conditions for the development of the artificial intelligence industry in the future.

## 5. CONCLUSION

Artificial intelligence has developed rapidly in recent years, leading to intense tensions related to personal privacy when businesses apply this technology to their retail operations. Understanding today's problem, our research proposes recommendations for governments of developing countries with similar economic conditions to Vietnam to refer to in the process of developing privacy protection policies. consumer privacy without being too strict on businesses. This study is a premise for further research on privacy in the context of an increasingly rapidly developing digital technology-based economy.

**ACKNOWLEDGMENTS**

The author gratefully acknowledges the financial support from the Banking Academy of Vietnam.

**CONFLICT OF INTEREST:**

The authors declare no conflicts of interest.

**AUTHOR CONTRIBUTIONS:**

Phan Dang Hai: Ideation, Conceptualization; Data search, Data analysis, Supervision, Writing - review and editing; Writing - preparing the original draft.

Nguyen Thi Mai Dung: Ideation, Conceptualization, Data search, Data management, Formal analysis; Writing - preparing the original draft

Nguyen Thai Ha: Methodology, Data analysis, Writing - Review and editing, proofreading.

Nguyen Thi Hue: Data search, Data analysis, Supervision, Writing – review.

**Journal of Information Systems Engineering and Management**
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

**DATA AVAILABILITY STATEMENT:**

The data presented in the study were collected from many different sources: (i) the author collected it himself through research published in prestigious scientific journals; (ii) annual reports are available upon request from the authors.

## REFERENCES:

[1] Ani Petrosyan (2024), *Average cost of a data breach in the United States from 2006 to 2023* (in million US dollars).
[2] Asuncion Esteve (2017), *The business of personal data: Google, Facebook, and privacy issues in the EU and the USA*, accessed on March 24, 2024;
[3] Auxier, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erica Turner (2019), How Americans Think About Privacy and the Vulnerability of Their Personal Data, *Pew Research Center*. November 15.
[4] Center for Data innovation (2021), Who is winning the AI race: China, The EU, or The United States? Available online: https://www2.datainnovation.org/2021-china-eu-us-ai.pdf ;
[5] Cisco (2024), *Privacy as an Enabler of Customer Trust*, available online: accessed on March 30, 2024;
[6] Chao Wang, Jieyu Zhang, Nicholas Lassi andXiaohan Zhang (2022), *Privacy Protection in Using Artificial Intelligence for Healthcare: Chinese Regulation in Comparative Perspective*. Available online: https://doi.org/10.3390/ healthcare10101878, (accessed on March 24, 2024);
[7] Federal Trade Commission (2023), *FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests*, accessed on April 12, 2024;
[8] Federal Trade Commission (2023), *Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Implemented Technology without Reasonable Safeguards,* accessed on March 12, 2024;
[9] Forbes Advisor (2023), *24 Top AI Statistics And Trends In 2024*, accessed on May 6, 2024);
[10] Forbes Advisor (2023), *How Businesses Are Using Artificial Intelligence In 2024*. Available online: accessed on May 6, 2024;
[11] Gabriele Pizzi, Daniele Scarpi (2020), *Privacy threats with retail technologies: A consumer perspective*, available online accessed on March 30, 2024;
[12] General Data Protection Regulation (2018). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2018*, available online: accessed on March 24, 2024).
[13] Government (2018), *Decree No. 01/ND-CP, dated August 6, 2018, stipulates the functions, tasks, powers, and organizational structure of the Ministry of Public Security*;
[14] Government (2020), *Decree No. 15/2020/ND-CP stipulating administrative sanctions in the fields of postal services, telecommunications, radio frequencies, information technology, network information security, and electronic transactions*.
[15] Government (2021), *Decision No. 127/QD-TTg by the Prime Minister: Issuing the National Strategy on Research, Development, and Application of Artificial Intelligence until 2030*.
[16] Government (2023), Decree No. 13/2023/ND-CP on Personal Data Protection.
[17] Government (2023), Decree No. 13/2023/ND-CP on Personal Data Protection;
[18] IBM (2022), *IBM Global AI Adoption Index 2022*, available online: accessed on May 1, 2024;
[19] Institute of Policy and Development Research in Communication (IPS), *Report Cross-Border Personal Data Transfer - From Trust to Freedom*;
[20] Kelly D. Martin, Robert W. Palmatier (2020), Data Privacy in Retail: Navigating Tensions and Directing Future Research, *Journal of Retailing*, Volume 96, Issue 4, December 2020, Pages 449-457, available online: accessed on March 25, 2024;
[21] Lemon, Katherine N. and Peter C. Verhoef (2016), "Understanding Customer Experience Throughout the Customer Journey," *Journal of Marketing*, 80 (November), 69–96;
[22] Luis Montezuma, The case for a hybrid model on data protection/privacy. available online: accessed on March 22,2024;

[23] Mc Carthy, J.; Minsky, M.L.; Rochester, N.; Shannon, CE A proposal for the Dartmouth Summer Research Project on Artificial Intelligence. *AIMag*. 2006 , *27*, 12.
[24] Minister of Information and Communications (2023), *Decision No. 1499/QD-BTTTT dated August 14, 2023, by the Minister of Information and Communications*, specifying the functions, tasks, powers, and organizational structure of the Department of Information Security;
[25] Ministry of Finance (2023), *High expectations for the retail market in 2023*. Available online: accessed on April 30, 2024
[26] Ministry of Information and Communications (2022), *Annual Report for the year 2022, directions, and tasks for 2023*;
[27] Ministry of Information and Communications (2023), *Annual Report for the year 2023, directions and tasks for 2024;* Part V. Network Information Security, Section 1.1, Page 52.
[28] Ministry of Public Security (2020), *Report on the Current State of Personal Data Protection*. Available online: accessed on March 1, 2024.
[29] Ministry of Public Security (2020*), Report on the Current State of Personal Data Protection*.
[30] Multistakeholderism, and the (Ir)relevance of the TBT Regime 51(2) Cornell *International Law Journal* (2018), at 445;
[31] National Assembly (2005), *Trade Law of 2005*. Available online: https://chinhphu.vn/default.aspx?pageid=27160&docid=14765 ;
[32] National Assembly (2013), *Constitution of 2013*.
[33] National Assembly (2015), *Civil Code of 2015*. Available online: https://vanban.chinhphu.vn/?pageid=27160&docid=183188 ;
[34] National Assembly (2015), *Law on Network Information Security of 2015*. Available online : https://vanban.chinhphu.vn/?pageid=27160&docid=183196 ;
[35] National Assembly (2015), *Penal Code of 2015*. Available online: https://vanban.chinhphu.vn/default.aspx?pageid=27160&docid=183216 ;
[36] National Assembly (2018), *Cybersecurity Law of 2018*. Available online: https://vanban.chinhphu.vn/?pageid=27160&docid=206114 ;
[37] National Assembly (2023), *Consumer Rights Protection Law of 2023*.
[38] Office of the United States Trade Representative. *US-Japan Digital Trade Agreement*.
[39] Oxford Insights (2022), *Government AI Readiness Index 2022*.
[40] Peng, Shin-yi (2018) ""Private" Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime," *Cornell International Law Journal,* Vol. 51 : No. 2 , Article 4.
[41] Petro, Greg (2019), "*Retailers Walking a Tightrope Between Data Privacy and Personalization,"* Forbes, May 17, (accessed April 24, 2024).
[42] Shin Yi Peng, 'Cybersecurity Threats and theWTO National Security Exceptions' 18 Journal of International; Szabó 2005. p. 46;
[43] The Leader (2023), *Artificial intelligence is changing the retail industry*. Available online: accessed on May 6, 2024;
[44] VnEconomy (2024) *Mobile World's revenue decreased sharply after closing hundreds of stores nationally*. Available online: accessed on April 11, 2024 );
[45] Warren, SD, Brandeis, LD: The Right to Privacy. *Harvard Law Review*, Volume 4, Issue 5. (1890) page 193;
[46] Wired (2024), The WIRED Guide to Your Personal Data (and Who Is Using It). Available online: accessed on March 24, 2024;
[47] World Economic Forum (2024), *Unlocking the Value of Personal Data February 2023*, Available online: accessed on March 24, 2024.