

To cite this article: Nguyen Thi Hoi and Tran Thi Nhung (2025). FACTORS AFFECTING INTENTION TO PROTECT PERSONAL DATA ON CYBERSPACE OF STUDENT, International Journal of Education and Social Science Research (IJESSR) 8 (2): 10-23 Article No. 1031, Sub Id 1615

FACTORS AFFECTING INTENTION TO PROTECT PERSONAL DATA ON CYBERSPACE OF STUDENT

Nguyen Thi Hoi and Tran Thi Nhung

Thuongmai University, Faculty of Economic Information System and E-commerce,
79 Ho Tung Mau Street, Cau Giay District, Hanoi, Vietnam

DOI: <https://doi.org/10.37500/IJESSR.2025.8202>

ABSTRACT

The rapid growth of information technology and online applications has made users increasingly dependent on internet-based services and platforms. Consequently, personal data is now more susceptible to loss, manipulation, and unauthorized access. To explore the factors influencing users' intentions to safeguard their personal data and offer recommendations for improving data security, a study was conducted using the Theory of Planned Behavior (TPB) and the Information Security Assurance model. The research model was tested with data from 434 internet users who are student at universities of Vietnam. The results showed that Risk Perception (0.318) had the greatest influence on users' intentions to protect their data, followed by Perceived Behavioral Control (0.284), User Attitude (0.264), and Subjective Norms (0.254), all of which were positively correlated with users' intentions. These findings highlight the importance of risk awareness, behavioral control, and individual attitudes in shaping personal data security practices online. This understanding helps internet users become more aware of privacy issues, contributing to the development of a culture that emphasizes personal data protection within the online community and raising individual responsibility for safeguarding their own data and that of others.

KEYWORDS: personal data, cyber security, risk perception, TPB.

1. INTRODUCTION

The rapid development of information technology, particularly the Internet and mobile devices, has generated vast amounts of personal data, making it a prime target not only for businesses and organizations but also for scammers, impersonators, and creators of fake news [4]-[16]-[26]. In Vietnam, as the country becomes increasingly integrated into the global economy, the protection of personal data has become an urgent necessity for the sustainable development of both society and the economy [6]-[35]-[28]-[30].

According to [34], data encompasses not only the content of information communicated but also the methods and conditions of communication, serving as a foundation for forming concepts, beyond merely describing the value of things and phenomena. [27] defines personal data as any information

related to an identifiable or potentially identifiable individual. Securing personal data, as described by [4], involves protecting it from unauthorized access, use, destruction, or alteration. The aim of personal data protection, according to [24]-[29], is to ensure confidentiality, integrity, authenticity, and availability of the data.

Data protection models have evolved as people sought to conceal information, such as in letters and orders [9]. For example, [12] developed processes to ensure secure communication between users, while [13] emphasized the importance of maintaining data integrity, availability, and accessibility. [37] introduced the Zero Trust model, focusing on centralized security and system reliability, and [22] proposed a model for managing rights to create, manage, delete, secure, transfer, and anonymize user data.

The concept of personal data protection, often referred to as Data Privacy, involves practices, regulations, and laws designed to prevent unauthorized alteration, copying, deletion, access, disclosure, or misuse of personal information [23]-[36]. Globally, many countries have enacted laws to address data privacy, including the European Union's General Data Protection Regulation (GDPR) [9], California's Consumer Privacy Regulation (CCPA) [27], Brazil's General Data Protection Law (LGPD) [20], and South Africa's Protection of Personal Information Act (POPIA) [11].

In Vietnam, the protection of personal data has become increasingly important in the context of the country's ongoing digital transformation. The government's Decree 13/2023/ND-CP on personal data protection sets standards for the processing of personal data [14]. Other related laws include the Cybersecurity Law (24/2018/QH14), the Law on Network Information Security (86/2015/QH13), and various decrees and circulars. These regulations are overseen by the Ministry of Information and Communications and the Ministry of Public Security.

In the digital era, safeguarding personal data is critical to ensuring trust in information systems and provides opportunities for business expansion while driving innovation and development [23]-[15]-[17]. Compliance with data protection regulations fosters technological and service innovation, enabling organizations to meet legal requirements and enhance trust in their business activities [17]-[16]-[21]. Ensuring personal data security not only protects individuals but also helps build consumer confidence in digital products and services, which is essential for the growth of the digital economy [24]-[26]-[31].

However, Vietnam faces significant challenges in personal data protection [30] – [36]. Data breaches and loss of control over personal information are on the rise, especially in the face of rapid digitalization and internet expansion [36] – [30] – 28].

Given the growing concern about personal data security among internet users, this article aims to identify the factors influencing individuals' intentions to protect their personal data online, proposing

solutions to enhance data protection in the digital space. The article is structured as follows: Introduction, theoretical foundation and research model, research findings, implications, and conclusion. Maritime industry.

2. Theoretical Basis and Propose Model

2.1. Related works

The study draws on the Theory of Planned Behavior (TPB) model, as proposed by [2] and [1], to examine the relationships between beliefs, attitudes, behavioral intentions, and actions. In the context of personal data protection, individuals' beliefs and perceptions are key factors in determining whether or not personal data in cyberspace is safeguarded. For this reason, TPB serves as the foundation for constructing the research model. Additionally, the study builds upon previous research related to personal data protection and online privacy to inform its model.

For example, [29] proposed a TPB-based research model to study the protection of patient data in electronic health records, examining nurses' behavioral intentions regarding data privacy. Their findings indicated that Attitude, Subjective Norms, and Perceived Behavioral Control directly influenced nurses' intentions. Similarly [17], also using TPB, explored factors affecting users' intentions to disclose personal data. Their results revealed that Perceived Benefits, Perceived Risks, Privacy Attitudes, and Subjective Norms influenced these intentions.

[39] combined TPB with computational theory to identify factors affecting users' privacy disclosures on social networking sites. They found that disclosure decisions were driven by privacy concerns and perceived benefits, with key factors including Behavioral Control, Subjective Norms, and Attitude. [10] applied the TPB model to predict safety behaviors in online services, concluding that Attitude, Subjective Norms, and Behavioral Control significantly influenced those behaviors. Similarly, [32] developed a TPB-based model to explain individuals' willingness to provide personal data to others or organizations, showing that Personal Data Security Risk Perception had the strongest impact on personal data security.

Additionally, [15] combined TPB with Privacy Calculus Theory and the Heuristic-Systematic Model to explore factors influencing users' information-sharing behavior on social networks. They identified key factors such as Security Background Knowledge, Information Deficiency, Information Search, Systematic Information Processing, and Risk Perception as influences on this behavior.

Based on these findings, the current study builds on the TPB model and relevant data security theories. It focuses on four main factors: Attitude, Subjective Norms, Perceived Behavioral Control, and Risk Perception, which are seen as key determinants of personal data protection behavior.

2.2. Proposed Model

2.2.1. Attitude

In the TPB model [1]-[2], attitude is recognized as a significant determinant of behavioral intentions. Numerous studies [10]- [29]-[39] have highlighted the crucial role of attitude in influencing personal data protection behaviors. When users have a positive attitude toward privacy protection measures, they are more likely to actively engage in safeguarding their personal data. Moreover, the influence of people around them such as family, friends, and colleagues also directly impact their behaviors. They highlight how the rapid growth of online services increases users' vulnerability, making their attitudes toward data protection even more critical [4]-[13]-[22]. Since personal data is highly susceptible to breaches and misuse, users' attitudes significantly affect their intention to protect their data [24]-[26]. Therefore, attitude is a key factor that positively influences the intention to protect personal data in cyberspace.

H1: User attitudes positively influence the intention to protect personal data in cyberspace.

2.2.2. Subjective Norms

Subjective norms refer to the social pressure an individual feels when deciding whether to engage in a particular behavior [1]-[2]. This pressure is often shaped by the cultural environment, family, friends, and colleagues. Subjective norms influence the perceived risks users consider before deciding to disclose their personal information [29] – [13] – [26]. For instance, if individuals believe those around them value privacy, they may be more inclined to use complex passwords or regularly update their privacy settings. Ajzen [2] and Fishbein & Ajzen [1] emphasize that alignment between personal attitudes and societal expectations can significantly impact the adoption of privacy-protecting behaviors. Further studies suggest that a strong combination of internal beliefs and external social influences shapes online behavior [4] – [10] – [13] – [24]. This indicates that promoting both individual attitudes and social expectations can enhance personal data protection. Therefore, the stronger the subjective norms, the greater the intention to protect personal data, making subjective norms a key element of the research model.

H2: Subjective norms positively impact the intention to protect personal data in cyberspace.

2.3. Perceived Behavioral Control

The TPB model suggests that the perceived ease or difficulty of performing a behavior influences an individual's intentions and actions [1]-[18]. Studies by [5] – [10]- [32] -[29] have identified perceived control over personal data as a key factor influencing users' behaviors in providing or protecting their information. When users feel more in control of their data, they are more likely to engage in protective behaviors [3] – [5] – [7] – [14] – [25]. In today's context of rapidly expanding social networks, users with greater control over privacy settings such as limiting unauthorized access perceive higher levels of behavioral control. This perception directly influences their intention to protect personal data. Therefore, perceived behavioral control is an important factor included in the research model.

H3: Perceived behavioral control positively impacts the intention to protect personal data online.

2.4. Risk Perception

Research by [17] – [32] – [15] – [35] – [31] indicates that risk perception related to data privacy significantly increases users' awareness and motivates protective behaviors in cyberspace. Users who perceive higher risks to their personal data are more likely to adopt protective measures. As digital platforms evolve and the complexity of threats increases, risk perception becomes an essential factor in motivating users to stay informed about data security issues [4] – [24] – [26]. Greater awareness of risks not only encourages stricter privacy practices but also motivates users to educate themselves and others on safe digital practices. Therefore, risk perception is a key factor in the research model.

H4: User risk perception positively impacts the intention to protect personal data in cyberspace.

Thus, the study proposes a research model based on TPB and studies identifying factors affecting users' intention to protect personal data in cyberspace as shown in Figure 1

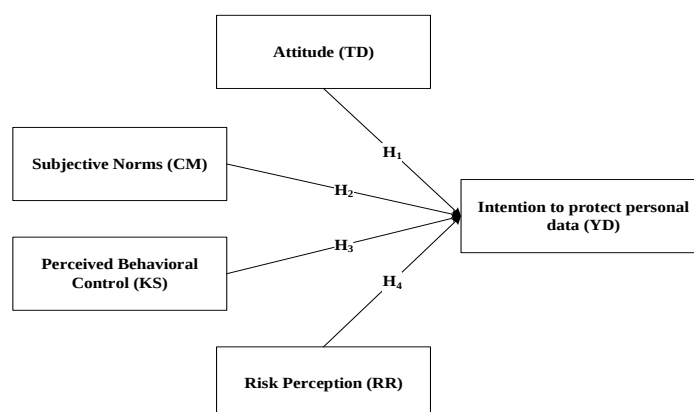


Figure 1: The proposed model

3. METHODOLOGY

3.1. Research process

The study employed a combination of qualitative and quantitative methods to develop a set of 24 survey questions based on the factors in the Theory of Planned Behavior (TPB) model and related studies. Data was collected from 434 individual consumers who have personal accounts and actively engage in social media activities. The data was then analyzed using Stata, SPSS, and AMOS software. The research process followed these steps: establishing the research foundation → developing a theoretical framework → conducting quantitative research (including Cronbach's Alpha reliability assessment → Exploratory Factor Analysis (EFA) → multiple linear regression analysis) → assessing

the reliability of the scale and testing hypotheses. Based on the findings, the study proposes research implications and solutions for both individuals and organizations.

3.2 Developing the Study Questionnaire

The questionnaire for the research model was developed based on the hypotheses and findings from previous studies. It included 21 scales, with 17 scales measuring influencing factors and 4 scales focused on the intention to protect personal data in cyberspace. The questionnaire consisted of two sections: The first section measured agreement levels using 24 statements with a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). The second section collected demographic information to support descriptive analysis and evaluate the factors affecting the intention to protect personal data in cyberspace.

4. Research Results and Discussion

4.1. Descriptive statistics

The study conducted an online survey via Google Forms, targeting users with personal accounts who regularly interact on the internet through various platforms, including social media, e-commerce websites, payment gateways, transaction portals, and search engines. A total of 450 responses were collected, and after preliminary data processing, 434 valid responses were retained for analysis. Among the participants, 65% were male and 35% were female, suggesting that at the time of the survey, men showed greater awareness and concern for personal data protection online compared to women.

Regarding age distribution, 77.5% of respondents were between 19 and 35 years old, 12.5% were between 36 and 59 years old, 9.2% were under 18, and only 0.8% were over 60. The participants' education levels were also significant, reflecting their awareness and understanding of privacy protection. Those with university degrees or higher made up 86.3% of the sample, while individuals with college or vocational training accounted for 10.4%, and 3.3% had a high school education. In terms of employment, 62.9% of the respondents were employed, 32.9% were students, and the remaining 4.2% belonged to other categories. These figures suggest that more educated and working individuals were more concerned about personal data protection in cyberspace.

4.2. Cronbach's Alpha Test

The study assessed the reliability of the scales using Cronbach's Alpha. The results, as shown in Table 1, indicate that all the Cronbach's Alpha coefficients were above 0.6, with TD = 0.795, CM = 0.758, KS = 0.751, RR = 0.756, and the Dependent Factor = 0.786. Additionally, all observed variables had a variable-total correlation coefficient greater than 0.3. These results confirm that the scales are reliable and of good quality, meeting the criteria for further analysis [19].

Table 1: The Cronbach's Alpha Coefficient

<i>Independent Variables</i>	<i>Observed Variables</i>	<i>Variable-Total Correlation Coefficient</i>	<i>Cronbach's Alpha Coefficient</i>
Attitude	Cronbach's Alpha = 0.795		
	TD1	0.597	0.749
	TD2	0.494	0.782
	TD3	0.582	0.754
	TD4	0.576	0.756
	TD5	0.632	0.739
Subjective Norms	Cronbach's Alpha = 0.758		
	CM1	0.556	0.701
	CM2	0.596	0.678
	CM3	0.525	0.717
	CM4	0.543	0.708
Perceived Behavioral Control	Cronbach's Alpha = 0.751		
	KS2	0.544	0.694
	KS2	0.534	0.700
	KS3	0.522	0.707
	KS4	0.586	0.672
Risk Perception	Cronbach's Alpha = 0.756		
	RR1	0.594	0.676
	RR2	0.562	0.694
	RR3	0.550	0.700
	RR4	0.505	0.724
Intention to protect personal data in cyberspace	Cronbach's Alpha = 0.786		
	YD1	0.624	0.717
	YD2	0.593	0.734
	YD3	0.570	0.745
	YD4	0.585	0.737

4.3 Exploratory factor analysis EFA

Next, the study conducted a test using the KMO and Bartlett's coefficients for the variables. The results in Table 2 show that the KMO index = $0.837 > 0.5$ and the Bartlett test = 1183.218 with a significance level of Sig. = $0.000 < 0.05$, which means that the variables are correlated with each other and meet the necessary conditions for factor analysis. The results of the factor analysis of "Intention to protect personal data" show that the KMO coefficient = $0.789 > 0.5$ and the significance level of Sig. = $0.000 < 0.05$, so it can be concluded that the factor analysis for the scales is consistent with the actual data.

Table 2: The Cronbach's Alpha Coefficient

<i>Com</i>	<i>Initial Eigenvalues</i>			<i>Extraction Sums of Squared Loadings</i>		
	<i>Total</i>	<i>% of Variance</i>	<i>Cumulative %</i>	<i>Total</i>	<i>% of Variance</i>	<i>Cumulative %</i>
1	2.438	60.947	60.947	2.438	60.947	60.947
2	.551	13.778	74.726			
3	.547	13.677	88.403			
4	.464	11.597	100.000			

In **Table 3**, it shows that the percentage of explained variance (Percentage of Variance) reaches 57.939%, higher than 50%, factor analysis is able to explain 57.939% of the total variation. At the same time, Eigenvalues has a coefficient of $2.438 > 1.0$, total extracted variance (Cumulative %) = $60.947\% > 50\%$), proving that 60.947% of the variation in the data is explained by the observed variables in Table 3.

Table 3: The Cronbach's Alpha Coefficient

<i>Co</i>	<i>Initial Eigenvalues</i>			<i>Extraction Sums of Squared Loadings</i>			<i>Rotation Sums of Squared Loadings</i>		
	<i>Total</i>	<i>% of Variance</i>	<i>Cumulative %</i>	<i>Total</i>	<i>% of Variance</i>	<i>Cumulative %</i>	<i>Total</i>	<i>% of Variance</i>	<i>Cumulative %</i>
1	4.815	28.326	28.326	4.815	28.326	28.326	2.784	16.378	16.378
2	1.814	10.669	38.996	1.814	10.669	38.996	2.391	14.065	30.443
3	1.687	9.926	48.921	1.687	9.926	48.921	2.347	13.807	44.250
4	1.533	9.018	57.939	1.533	9.018	57.939	2.327	13.689	57.939
5	.817	4.809	62.748						
6	.746	4.390	67.138						
7	.704	4.141	71.279						
8	.628	3.694	74.972						
9	.622	3.656	78.628						
10	.563	3.315	81.943						
11	.519	3.055	84.998						
12	.506	2.977	87.975						
13	.465	2.733	90.708						
14	.448	2.635	93.344						
15	.428	2.518	95.862						
16	.372	2.188	98.050						
17	.331	1.950	100.000						

After conducting exploratory factor analysis, the results showed that 17 observed variables can be divided into 4 factor groups in Table 4 with Factor Loading > 0.5. This shows that the analyzed data is suitable and regression analysis can be conducted for the model.

Table 4: Rotated Component Matrixa

	<i>Component</i>				<i>5</i>
	<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	
TD5	.782				
TD4	.734				
TD1	.706				
TD2	.678				
TD3	.675				
RR1		.808			
RR3		.713			
RR2		.706			
RR4		.695			
CM2			.771		
CM1			.752		
CM4			.720		
CM3			.679		
KS2				.762	
KS1				.753	
KS4				.712	
KS3				.709	
YD1					.805
YD2					.781
YD4					.774
YD3					.762

4.4. Correlation analysis

The study conducted a correlation analysis between the independent and dependent variables, giving the results in Table 5. The results show that all 4 independent variables have Sig. = 000 < 0.05. Thus, there is a correlation between the dependent variable and the independent variable, or the 4 independent variables (TD; CM; KS; RR) all have a positive correlation with the dependent variable YD.

Table 5: Pearson correlation analysis table

		<i>YD</i>	<i>TD</i>	<i>CM</i>	<i>KS</i>	<i>RR</i>
YD	Pearson Correlation	1	,525**	,526**	,509**	,559**
	Sig. (2-tailed)		,000	,000	,000	,000
	N	434	434	434	434	434

4.5. Regression analysis

After performing regression analysis with variables TD; CM; KS and RR. The significance level was set at 5%. meaning the confidence level was 95%. The results showed in Table 6 that the value of R = 0.759, meaning that there is a close relationship between the variables in the model, the value of R Square = 0.576 indicates that YD is explained by 4 influencing factors TD, CM, KS and RR. Thus, the regression model satisfies the conditions and tests the suitability of the research model. The F test used and through the ANOVA analysis of variance table shows that the value of F = 79.746 has a Sig. = 0.000 < 0.5, meaning that the regression model is suitable for the collected data and the variables included are all statistically significant.

Table 6: Rotated Component Matrixa

<i>Model</i>		<i>Unstandardized Coefficients</i>		<i>Standardized Coefficients</i>	<i>t</i>	<i>Sig.</i>	<i>Collinearity Statistics</i>	
		<i>B</i>	<i>Std. Error</i>	<i>Beta</i>			<i>Tolerance</i>	<i>VIF</i>
1	(Constant)	-.359	.232		-1.546	.123		
	TD	.264	.051	.247	5.145	.000	.785	1.273
	KS	.282	.049	.268	5.808	.000	.845	1.183
	CM	.254	.048	.251	5.258	.000	.789	1.267
	RR	.321	.047	.318	6.763	.000	.819	1.221

The results in Table 7 show that 4 variables are included in the regression analysis model, all of which have Sig.=0.000 < 0.05, meaning that all independent variables have a relationship with the dependent variable, or hypotheses H1, H2, H3, H4 are all accepted in the model, from which we have:

Unstandardized regression equation ($YD = 0.264*TD + 0.282*KS + 0.254*CM + 0.321*RR + e$) and the regression equation after standardization: ($YD = 0.318*RR + 0.268*KS + 0.251*CM + 0.247*TD + \square$). The results of the regression equation on the normal distribution line show in Figure 2, Figure 3, the mean value Mean = $1.07e-15$ approximately = 0, standard deviation = 0.992 approximately = 1, it can be concluded: The normal distribution assumption of the residual is not violated. In addition, the normal distribution residual is concentrated around the abscissa 0, so the linear relationship assumption is not violated. It can be concluded that the 4 hypotheses in the model are all accepted.

From the test results, it can be seen that, when not considering other factors, the relationship between Attitude, Subjective Norm, Level of Behavioral Control, Risk Perception and Intention to Protect Personal Data is in the same direction.

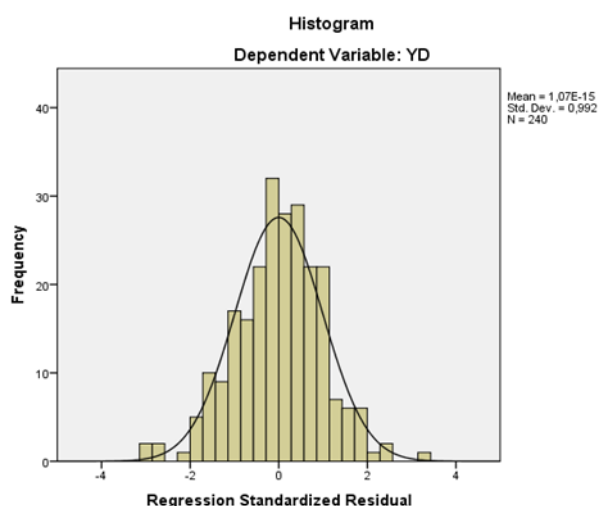


Figure 2: Histogram of model

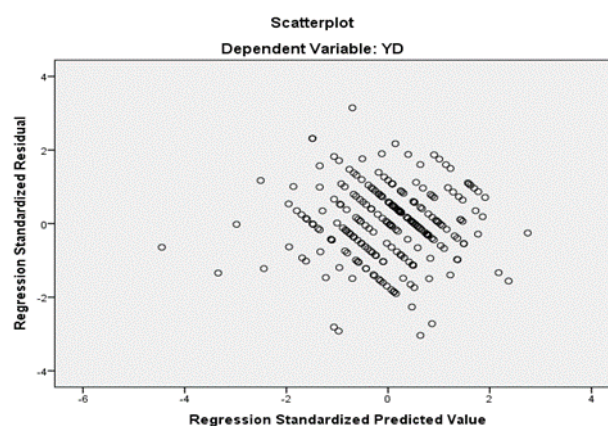


Figure 3: Scatterplot of model

5. CONCLUSION AND IMPLICATIONS

Research on the factors influencing the intention to protect personal data during Vietnam's digital transformation period holds great significance for online users. The study's findings highlight that users are increasingly concerned about risks in cyberspace ($RR = 0.318$). This growing concern underscores the importance for organizations and businesses providing online services to regularly implement measures and enhance solutions to safeguard user privacy and prevent data loss.

Secondly, the influence of subjective norms ($CM = 0.268$) indicates that individuals place a higher value on personal privacy, creating opportunities to educate and promote privacy awareness. This helps users remain vigilant and reduce the potential damages caused by data breaches in cyberspace.

Third, the effect of perceived behavioral control ($KS = 0.251$) demonstrates that when users feel they have more control over their personal data in cyberspace, they are more likely to adopt behaviors that

protect their privacy. As a result, they are not only more cautious but also more likely to voluntarily implement privacy protection measures in their online activities.

Lastly, attitude ($TD = 0.247$) plays a crucial role, as supported by the research of [2]-[1], who confirmed that attitude significantly influences behavioral intentions. In the context of personal data protection, users' attitudes are pivotal in ensuring the safety of their data online. Thus, it is essential to encourage and foster positive attitudes toward privacy protection measures provided by organizations, application systems, and services. Simplifying and facilitating the adoption of these measures will make it easier for users to implement them, enhancing their data security.

The study's results align with previous research by [10] – [15] – [17], this research not only contributes to theoretical understanding but also aids in developing effective personal data protection strategies and policies that are aligned with Vietnam's digital transformation. By identifying key influencing factors, the study provides valuable insights for managers, businesses, and social organizations to create a safer, more transparent, and trustworthy digital environment. Additionally, it helps online users better understand privacy issues, fostering a culture of personal data protection and raising individual awareness and responsibility in safeguarding their own data as well as that of others.

6. Acknowledgment

We extend our gratitude to the student groups who support the data collection for this study. This research is funded by Thuongmai University, Hanoi, Vietnam. Thank you very much.

REFERENCES

- [1] Ajzen, I. and Fishbein, M. (1980). Understanding Attitudes and Predicting Social Behavior. Prentice-Hall, Englewood Cliffs
- [2] Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes, 50(2), 179-211.
- [3] Aleksandar K., Samuel C. & Jasna M. (2024, Jan 23). U.S. Data Privacy Laws in 2024: State and Federal Laws That Protect Your Data. <<https://www.cloudwards.net/us-data-privacy-laws/>>
- [4] Alharbi N. N. A., Yanhui Li (2020). Impacts of Trust in Government and Privacy Risk Concern on Willingness to Provide Personal Information in Saudi Arabi, International Journal of Management Science and Business Administration, 6(2), 7-1
- [5] Alzighaibi, Ahmad. (2021). Cybersecurity Attacks on Academic Data and Personal Information and the Mediating Role of Education and Employment. Journal of Computer and Communications. 09. 77-90. 10.4236/jcc.2021.911006.
- [6] Anh, N. (2024). Towards the goal of “cyber security superpower”. VnEconomy. Retrieved March 19 from <https://vneconomy.vn/huong-toi-muc-tieu-cuong-quoc-an-toan-thong-tin-mang.htm>
- [7] Bach Thi Nha Nam. (2022). Building the concept of personal data in Vietnamese law referring to the experience of the European Union. Journal of State and Law (6).
- [8] Ben W. (n.d.). What is GDPR, the EU's new data protection law? <<https://gdpr.eu/what-is-gdpr/>>

- [9] Bennett, C. J. (1992). Regulating privacy: Data protection and public policy in Europe and the United States. Cornell University Press.
- [10] Burns, S., & Roberts, L. (2013). Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety*, 15, 48-64.
- [11] Cookiebot. (2021, July 1). POPIA – South Africa Data Protection. <<https://www.cookiebot.com/en/popia/>>
- [12] Coron, J. S. (2006). What is cryptography? *IEEE security & privacy*, 4(1), 70-73.
- [13] Cherdantseva, Y., & Hilton, J. (2012). The Evolution of Information Security Goals from the 1960s to today. Unpublished. February.
- [14] Government of Vietnam (2023, May 17). Decree No. 13/2023/ND-CP: Protecting personal data rights; preventing personal data infringements. <<https://xaydungchinh sach.chinhphu.vn/nghe-dinh-so-13-2023-nd-cp-bao-ve-quyen-du-lieu-ca-nhan-ngan-chan-cac-hanh-vi-xam-pham-du-lieu-ca-nhan-119230513100359528.htm>>
- [15] Dung, N.V., & Tien, V.V (2023). Research on factors affecting information sharing behavior on social networks. *Journal of Information and Communication Technology Science*, 1, 27-40
- [16] Dvojmoč, Miha & Verboten, Mojca. (2022). Cyber (In)security of Personal Data and Information in Times of Digitization. *Medicine, Law & Society*. 15. 287-304. 10.18690/mls.15.2.287-304.2022.
- [17] Fan, A., Wu, Q., Yan, X., Lu, X., Ma, Y., & Xiao, X. (2021). Research on influencing factors of personal information disclosure intention of social media in China. *Data and Information Management*, 5(1), 195-207.
- [18] Fishbein, M., and Ajzen, I. (1975). Belief, attitude, intention and behavior: An introduction to theory and research. Reading, MA: Addison-Wesley.
- [19] Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E., & Tatham, R.L. (2010). *Multivariate Data Analysis*. Prentice Hall.
- [20] Heloisa V., CIPM (2024, Feb 14). Brazil's General Data Protection Law (LGPD) Explained. <<https://termly.io/resources/brazils-general-data-protection-law/>>
- [21] Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28(1), 65-98.
- [22] Huertas Celdrán, A., Gil Pérez, M., Mlakar, I., Alcaraz Calero, J. M., García Clemente, F. J., & Martínez Pérez, G. (2019, November). A management platform for citizen's data protection regulation. In *International Conference on Smart City and Informatization* (pp. 60-72). Singapore: Springer Singapore.
- [23] Juliette E. (2023, Aug 08). Data Privacy and Security: Safeguarding Information in the Digital age.
- [24] Kabay, M. E. (2002). What's Important for Information Security: A Manager's Guide. Norwich University, Northfield.

- [25] Kat MH Hille (2023, May 12). Vietnam's Personal Data Protection Decree: Overview, Key takeaways, and Context. Future of Privacy Forum. <<https://fpf.org/blog/vietnams-personal-data-protection-decree-overview-key-takeaways-and-context/>>
- [26] Kuner, Christopher & Svantesson, Dan & Cate, Fred & Lynskey, Orla & Millard, Christopher. (2017). The rise of cybersecurity and its impact on data protection. *International Data Privacy Law*. 7. 73-75. 10.1093/idpl/ix009.
- [27] Law, F., & Rights, F. (2006). On Personal Data. Hereinafter Referred to as the "Personal Data Law"..
- [28] Luu, Tran (2024). The challenge of protecting personal data in the cyberspace. Saigon Giai Phong, Retrieved July 07 from <https://www.sggp.org.vn/thach-thuc-bao-ve-du-lieu-ca-nhan-tren-khong-gian-mang-post749620.html>
- [29] Ma, C. C., Kuo, K. M., & Alexander, J. W. (2015). A survey-based study of factors that motivate nurses to protect the privacy of electronic medical records. *BMC medical informatics and decision making*, 16(1), 1-11.
- [30] Minh Son. (2021). Bkav continues to have hundreds of user data publicly disclosed by hackers. *Vietnam+*. 585
- [31] Möller, D. (2020). *Cybersecurity in digital transformation: Scope and applications*. Berlin/Heidelberg, Germany: Springer.
- [32] Quan, N.H., Xuyen, P.T., Thuy, N.T., & Anh, D.X.P. (2020) The impact of personal data protection factors on online consumer behavior. *Journal of Economics and Forecasting*, 77-81
- [33] National Assembly. (2018). *Law on Cyber Security*. National Assembly of the Socialist Republic of Vietnam.
- [34] Rick B. (2021, Sep 24). Complete Guide to LGPD: Brazil's Data Privacy Law. <<https://wirewheel.io/blog/lgpd-brazil-data-privacy-law-guide/>>
- [35] RiskXchange. (2023). Cybersecurity statistics you should know in 2023. RiskXchange. Retrieved March 19 from <https://riskxchange.co/1006415/cybersecurity-statistics-2023/>
- [36] Son, M. (2023). Cybersecurity: Notable trends in the last 6 months of 2023. *VietnamPlus*. Retrieved March 19 from <https://www.vietnamplus.vn/an-ninh-mang-nhung-xu-huong-dang-chu-y-trong-6-thang-cuoi-nam-2023-post869804.vnp>
- [37] Stafford, V. A. (2020). Zero trust architecture. NIST special publication, 800, 207.
- [38] Thuy Dieu. (2023). Minister To Lam: Cybersecurity must be a driving force for economic growth. *Vietnam Economic Times*. Venkataramanan, N., & Shriram, A. (2016). *Data privacy: principles and practice*. CRC Press.
- [39] Xu, F., Michael, K., & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: an integrated model. *Electronic Commerce Research*, 13, 151-168.