International Journal of Religion
2023
Volume: 4| Number 2 | pp. 166 – 172
ISSN: 2633-352X (Print) | ISSN: 2633-3538 (Online)
ijor.co.uk
DOI: https://doi.org/10.61707/613eg160

Online Personal Data Protection Focuses on The Path of Vietnam's Digital Transformation and The Next Stage

Nguyen Ngoc Anh Dao[1]

Abstract

Vietnam's rapid digital transformation has led to an exponential growth in online activities, generating vast amounts of personal data. As the country continues to evolve, ensuring the protection of this sensitive information has become a pressing concern. This study examines the current state of online personal data protection in Vietnam, highlighting the challenges and opportunities that arise from the nation's digital transformation. The study conducted a review to evaluate the personal data and privacy protection practices on e-government portals and e-service portals in Vietnam. In this study, based on two dimensions were assessed: (i) privacy policies issued by local governments; and, (ii) specific measures to implement such policies through technical tools. The findings indicate that while Vietnam has made significant strides in developing its digital infrastructure, the protection of personal data remains a significant challenge. The study identifies several key areas of concern, including inadequate legal frameworks, insufficient public awareness, and limited enforcement mechanisms. However, it also highlights opportunities for improvement, such as the potential for data protection regulations to drive innovation and economic growth. The study concludes by outlining a roadmap for the next stage of Vietnam's digital transformation, emphasizing the importance of robust data protection measures. It recommends the development of a comprehensive legal framework, increased public awareness campaigns, and enhanced enforcement mechanisms to ensure the effective protection of personal data. By addressing these challenges and seizing these opportunities, Vietnam can create a robust digital ecosystem that balances economic growth with individual privacy and security.

Keywords: *Online Personal Data Protection, Digital Transformation*

INTRODUCTION

Privacy is acknowledged as a fundamental right in Vietnam by the 2013 Constitution and other laws. Electronic provincial government portals (e-government portals - EGPs), online public service portals (e-service portals - ESPs), and smart applications (apps) are some of the tools that provincial-level People's Committees employ to collect a significant amount of personal information as the digital transformation of the public sector is accelerated. Nevertheless, the protection of personal data and the guarantee of user privacy on those interfaces have not been given the necessary attention. The policies of those platforms are still deficient in meeting the current legal requirements, particularly in comparison to best practices.

In this context, this study has recently conducted a review to assess the personal data and privacy protection practices of EGPs and ESPs in all 63 provinces, as well as apps that are being used in 50 provinces, based on the current legal framework (IPS & UNDP Vietnam 2022). Two dimensions were evaluated: (i) privacy policies implemented by local administrations; and (ii) specific technical instruments that were employed to enforce these policies. Key findings from the review are presented in this article. It also offers policy and practical recommendations for central and local government agencies on how to enhance the protection of personal data and privacy on online government-citizen interaction interfaces at the provincial level in Vietnam.

The Status of Online Personal Data Protection in Vietnam

In light of the increasing acquisition of sensitive data from citizens through digital government activities and the escalating hazard and cost of data breaches in the public sector, it is imperative to evaluate and supervise the personal data processing practices of government agencies. The objective of the review, which was conducted from May to April in 2024, was to enhance the awareness of personal data protection among local governments in Vietnam's digital environment. This was accomplished by examining the privacy policies and technical measures of three types of government-citizen interaction interfaces, including EGPs, ESPs, and apps,

[1] Faculty of Law and Economics, Ho Chi Minh University of Banking, Ho Chi Minh City, Vietnam. E-mail: daonna@hub.edu.vn

in all 63 provinces. Seventeen specific indicators were employed to conduct the review (United Nations in Viet Nam 2023), which include, inter alia, whether privacy policies specify government agencies responsible for protecting privacy; types of information collected by local governments; with which third-party agencies the personal information is shared; and children's privacy regulations. Below are key findings from the review.

Data Security and Personal Data Privacy Violations: Inevitable Risks to Manage

The digitalization of information and the public sector's e-services in Vietnam have led to the accumulation and concentration of sensitive data about citizens in the digital realm. (Vietnam Government 2023) The Ministry of Public Security (MPS) concluded the national population database in 2021 and is striving to achieve digital authentication of all personal identification accounts on ESPs at the national, ministerial, and provincial levels by 2022. (Cameron et al. 2019) The National Data Exchange Platform, which is comprised of 10 databases and eight information systems, has been established by the Ministry of Information and Communications (MIC). It is connected to over 90 ministries, sectors, provinces, and enterprises. In 2021, the Platform has facilitated 180,919,031 data transactions (Statista Market Insights 2024) (about 500,000 transactions per day), which helped increase data reuse and reduce duplications of data registration.

Consequently, it is imperative to mitigate the risks associated with data security and personal data privacy violations. During the initial stages of the COVID-19 pandemic, this tendency was readily apparent as the mainstream media and the authorities frequently disclosed the private information of COVID-19 carriers, such as their names, addresses, medical data, and private affairs. Between May 2020 and May 2021, the MPS recorded 2,500 instances of digital fraud. Of these, 527 instances involved criminals impersonating government officials and employing schemes to commit financial deception. Identity theft, which involves the counterfeiting or misuse of personal data, is on the increase, although the causal relationship between fraud cases and data breaches has not yet been established. By July 1, 2022, 50 million chip-based identity cards will be distributed to citizens, and the national population database will serve as the foundation for digital transactions. Consequently, identity fraud could have even more severe consequences.

In addition, there is additional evidence that Vietnam's public sector appears to be underperforming in term of data protection. The Vietnam Digital Transformation Index (DTI) in 2021 (Open Development Vietnam 2023) suggests that enhancing information security be one of the two priorities to improve digital government performance at both ministerial and provincial levels. The 2021 DTI's information security received low ratings of 0.2948 across ministries and 0.3267 across provinces on the 0-1-point scale, in comparison to other indicators such as digital transformation awareness, digital governance, and digital infrastructure.

Local Governments' Limited Awareness and Practice of Personal Data and Privacy Protection on Online Government-Citizen Interaction Interfaces

(Civil Code and the Law on Cyberinformation Security and Law on Electronic Transactions and the Law on Telecommunications) The review indicates that 59 out of 63 EGPs and 60 out of 63 ESPs have not yet published a Privacy Policy, which is a type of e-agreement that outlines the responsibilities of state agencies to safeguard citizens' data and establishes a legal foundation for citizens to exercise their personal data rights in the event of a data breach or personal data violation. Provincial policies and tools regarding personal data and privacy protection on EGPs, ESPs, and applications are considered to be spontaneous and have not been the result of explicit recognition of the significance of privacy.

Despite the fact that the documents on information security issued by the local governments are readily accessible online, they focus on technical requirements to ensure the safety and security of data, the prevention of cyber risks, and cyber security, rather than personal data privacy and users' privacy. In actuality, provincial-level state agencies have not prioritized personal data protection in a meaningful manner. 59 EGPs and 60 ESPs did not have any specific terms and conditions regarding personal data protection. The evaluation demonstrates that none of the 63 provinces have established a comprehensive standard for personal data protection. The majority of provincial interfaces necessitate users to verify the accuracy of the information they submit; however, they do not provide users with the means to articulate their privacy preferences.

The 2021 DTI findings indicate that the input factors, such as information technology facilities and infrastructure, have been given more attention in the context of privacy protection in the entire process of local government interaction with citizens in the digital environment (Open Development Vietnam 2023). Nevertheless, additional enhancements are necessary to the implementation of personal data and privacy protection policies and laws. In particular, the outputs, which encompass the extent to which personal data are safeguarded, have not satisfied the standards of the current legal framework. The quantity and quality of privacy policies are indicative of a lack of attention given to privacy policies, as illustrated in Table 1.

Table 1: Summary of policies on the data protection all provinces and city in Vietnam

Privacy policies on apps	Privacy policies on EGPs	Privacy policies on ESPs
Out of 32 provinces with privacy policies on their applications, only one (Hau Giang) designates the Provincial People's Committee as the agency responsible for data control. Out of the 32 provinces with applications, five (Binh Dinh, Da Nang, Dong Thap, Thua Thien-Hue, and Vinh Long) have implemented privacy policies that establish agreements between provincial Departments of Information and Communications (DICs) and users. Out of the 32 provinces with applications, eleven (Bac Kan, Bac Lieu, Ben Tre, Can Tho, Hoa Binh, Hung Yen, Kon Tum, Long An, Quang Nam, Quang Ninh, and Soc Trang) have implemented privacy policies that establish e-agreements between service providers and consumers. Fifteen of the 32 provinces (An Giang, Ba Ria-Vung Tau, Cao Bang, Hai Phong, Kien Giang, Lai Chau, Lang Son, Ninh Binh, Phu Yen, Son La, Tay Ninh, Thai Binh, Thai Nguyen, Tien Giang, and Vinh Phuc) did not specify which agency is responsible for safeguarding the privacy of data subjects; they simply stated "We."	The agency responsible for data acquisition and control is not accurately identified in four provinces that have announced privacy policies on EGPs: Binh Dinh, Phu Tho, Ha Noi, and Thua Thien-Hue.	An agreement between the DICs and consumers was established in one of the three privacy policies published on ESPs (Da Nang). (Open Development Vietnam 2023). An e-agreement between the service provider (WSO2 Identity Server) and consumers was established in one of the three privacy policies published on ESPs (Gia Lai). Out of the three privacy policies that are published on ESPs, one (Thua Thien-Hue) does not specify the agency that is liable for safeguarding the privacy of data subjects.

In particular, a total of 39 privacy policy documents were discovered across all three online interfaces of local administrations in 63 provinces, in terms of quantity. Of these, only three ESPs (Da Nang, Gia Lai, and Thua Thien-Hue) and four EGPs (Binh Dinh, Phu Tho, Ha Noi, and Thua Thien-Hue) have published privacy policies.

Of the 50 provinces whose apps are searchable on Google Play and Apple Store, 32 have included and publicized privacy policies, while the remaining 18 have either no privacy policy or a privacy policy that is inaccessible. The higher rate of privacy policy publication on apps in comparison to EGPs and ESPs can be attributed to the built-in technical requirements of Google Play and Apple Store, which mandate that app developers publish privacy policies upon the launch of their applications.

In terms of quality, none of the privacy policies that have been identified entirely meet the conditions outlined in the 2006 Law on Information Technology, Government Decree 64/2007/ND-CP, and MIC's Circular 25/2010/TT-BTTTT, as well as the six United Nations principles on personal data protection and privacy. The majority of the current privacy policies are unsuccessful in establishing effective e-contracts between the responsible government agencies (People's Committees of local governments) and data subjects (users of EGPs, ESPs, and the applications). Common confusion regarding the legal responsibilities of the government agencies (People's Committees of local governments), the operating agencies (DICs), and the service providers (private companies/individuals) is a result of the unclear attribution of the right to data control.

Misidentification of the responsible agencies will result in the failure to protect data subjects' rights by holding the responsible agencies accountable for their legal obligations, such as providing access, correcting or deleting data upon request, addressing administrative and judicial appeals, and communicating personal data breaches to data subjects, in order for privacy policies to establish a legal relationship between data subjects and the responsible government agencies. Only one of the 39 provincial privacy policies reviewed accurately identifies the provincial People's Committee as the agency responsible for determining the purpose and meaning of data

processing, and the DIC as the operating agency that processes personal data on behalf of the People's Committee. This information is drawn from the Hau Giang province app.

The contact mechanism, which is crucial for the establishment of digital contracts between local government agencies and data subjects, is another example of a poor practice. However, only eight of the 39 privacy policies offer official government emails, while 13 provide personal/business emails. The privacy policies of the apps of Can Tho and Quang Nam even shared the same contact email address (Open Development Vietnam 2023), which indicates that they have copied the policy from one another without an effort to localize the email contact.

Deficits In the Policy Framework and General Legislation Regarding Personal Data Protection

The review revealed a number of voids in the current policy and legal framework on personal data protection, as evidenced by the inadequacies in the practices of personal data and privacy protection on the online government-citizen interaction interfaces.

Initially, Vietnam has not yet established a distinct definition and classification of personal data in accordance with the latest digital transformation trends, which encompasses the categories of personal data that are collected from users on the interaction interfaces of the authorities. (National Assembly of the Socialist Republic of Vietnam, 2018) The definition of personal information in Government Decree 64/2007/ND-CP is too limited, whereas the 2018 Law on Cyber Security provides an overly comprehensive definition. Personal information that is routinely collected on the e-portals of government agencies is only mentioned in the MIC's Circular 25/2010/TT-BTTTT.

Secondly, the concepts of data privacy and privacy rights have not yet been adequately defined. The extant legal framework focuses more on technical requirements to assure data security than data privacy, as it was constructed prior to the emergence of personal data privacy protection as a social issue. Consequently, it appears that local governments are presently placing a greater emphasis on data security (government agencies versus external cyber threats) than on data privacy (government agencies versus data subjects).

Third, the legal framework and policy have not explicitly differentiated between the data controller and the data processor. Consequently, it is difficult to establish a precise definition of the liabilities of these entities with respect to data subjects. For instance, can the publication of a privacy policy document by a state agency serve as a foundation for establishing its liability regime? Or, in the event of a data breach, who is responsible for notifying users and providing compensation to data subjects? Furthermore, the legal relationship between state agencies that collect personal data and service providers that provide those online interfaces is unclear.

Fourth, the manner in which privacy protection is incorporated into the processes and procedures of storing, using, and sharing large volumes of personal data collected by state agencies is ambiguous. The detention period is the most common disparity.

Fifth, the law does not yet include regulations regarding personnel who serve as focal points for the preservation of personal data and privacy in the operations of state agencies. This is in addition to the specifications regarding the focal points' responsibilities and the necessity of disclosing their contact information as a component of the digital contract terms and conditions between state agencies and consumers of e-services or e-government portals.

Sixth, the public sector's mechanisms for handling violations, resolving complaints, lawsuits, compensation for harm, and sanctions related to personal data and privacy protection in the digital environment have not been clearly and specifically regulated. This fails to align with the rapidly evolving digital transformation trends and the requirements for the evolution of e-government.

Seventh, there is a dearth of specific regulations and guidelines that provinces must adhere to in order to more effectively safeguard the privacy and personal data of citizens in the digital environment. This has resulted in a lack of consistency among provinces regarding the protection of personal data and privacy in the online interactions between local governments and their citizens.

IMPLICATION AND DISCUSSION

Despite the Government of Vietnam's efforts to combat the illegal commercialization of personal data in the private sector, there has been a lack of attention devoted to the preservation of personal data privacy on Internet-based interfaces by government agencies at all levels. It is crucial that the central and local administrations in Vietnam prioritize the preservation of personal data in the public sector. The protection of personal data and the establishment of public trust in digital transformation will not only serve the purposes of digital governance but also contribute to the sustainable development of Vietnam's digital economy in the long term. This is due to the fact that digital identities, which are created, authenticated, and managed by the government, have become the foundation of digital economy activities. Additionally, personal data protection is incorporated into all new-generation digital trade agreements and digital economy partnership agreements. The following are critical recommendations based on the review's findings.

Improving the national regulatory framework for personal data and privacy protection in government-citizen interaction interfaces

When Vietnam reviews or develops legal documents that regulate government interfaces such as ESPs, EGPs, or other types of government-citizen interaction interfaces, the following six suggestions regarding the preservation of personal data and privacy must be taken into account at the national level:

It is necessary to explicitly define and categorize personal data in accordance with the most recent digital transformation trends, which encompasses the categories of personal data that are collected from users on government interfaces. Simultaneously, it is imperative to differentiate between data privacy and data security. Data privacy pertains to safeguarding personal privacy, whereas data security prioritizes the security of state agencies and the information technology system.

It is imperative to differentiate between data controllers and data processors in order to explicitly establish the legal obligations of these parties toward data subjects. For example, the regulatory framework must specify tools that enable individuals to exercise their rights to agree or disagree with the provision of personal information on government applications or interfaces, thereby establishing the default liability of state agencies when publishing privacy policy documents.

It is necessary to refine the provisions regarding the management of violations that occur during the processing of personal data by state agencies, officials, and civil servants. It is imperative to specify the types of violations and the corresponding sanctions. For instance, requirements for state compensation for government agencies' breaches of personal data protection, administrative, criminal, and civil processes and procedures for handling violations of personal data and privacy, and a focal agency to receive and process requests and complaints related to personal data should be established.

Provisions regarding the assignment of personnel responsible for the preservation of personal data and privacy in state agencies that are relevant to the matter should be included in laws, at the very least at the provincial level. The profile and contact information of this individual should be made public in order to facilitate communication between constituents and the individual in question. This individual is accountable for monitoring the compliance of local governments with legal regulations, common standards, and internal policies regarding privacy and personal data protection, providing guidance to local government agencies on the subject, and acting as a liaison between data subjects and governing bodies as required.

In order to ensure that personal data and privacy protection practices are consistent across all provinces, the MIC should create template privacy documents for local government agencies to implement when offering online public services. This will ensure that personal data and privacy protection are standardized. In addition, these shall encompass a sample contract between government agencies and service providers of government-to-citizen interaction interfaces, as well as a sample privacy policy and sample terms of use between the responsible government agencies and users.

Enhancing the protection of personal data and privacy in the local digital environment

The review indicates that local governments should prioritize three critical actions: the development of local action plans that are appropriate for their respective contexts, the implementation process, and the protection of citizens' rights and interests. Personal data and privacy protection policies, as well as practical instruments to implement those policies on interaction interfaces, must adhere to and satisfy all pertinent Vietnamese laws and regulations. In particular, it is imperative to establish a clear identification of the primary agencies, tools, and channels that are responsible for receiving remarks or complaints regarding personal data and privacy violations, as well as public feedback on the quality and efficacy of privacy protection.

Local governments must ensure that the rights and interests of citizens who utilize services, products, and tools on EGPs, ESPs, and applications are safeguarded. Consequently, it is imperative that local governments conduct regular assessments of their performance in this area to guarantee the enhanced protection of personal data and privacy. Additionally, local governments should be provided with specific measures and tools to ensure the legitimacy and lawfulness of processing personal information, collecting and using personal information for specific purposes, collecting personal information limited to stated purposes, specifying information storage duration, and increasing transparency and accountability in the collection, processing, storage, and use of personal information.

Assessing the efficacy of state agencies in protecting personal data and privacy on digital interfaces

It is suggested that the evaluation of government efficacy in the preservation of personal data and privacy be extended to all levels of government, rather than just local governments. The national digital transformation objectives and criteria for evaluating personal data protection should include indicators and targets on personal data and privacy protection for Vietnam's DTI.

Additionally, state agencies at all levels should conduct routine, comprehensive evaluations of their privacy protection practices and personal data. The review should not be restricted to EGPs, ESPs, and applications; it should also encompass databases administered by state agencies, where personal data are stored, used, and shared after being collected from interaction interfaces.

Implication On the Legal and Technical Aspects of Data Protection and The Future Plan of Legal Framework

By employing a comprehensive and multifaceted strategy that addresses both the legal and technical aspects of data protection, Vietnam can achieve a balance between the necessity for digital innovation and data protection. The following are several notable strategies:

Establish a Robust Legal Framework: Develop a legal framework that is both unified and resilient, defining personal data, outlining the rights of data subjects, and establishing explicit responsibilities for data controllers and processors. This framework should be updated on a regular basis to account for the changing nature of digital technologies and trends.

Increase Public Awareness and Education: Implement public awareness campaigns to inform citizens of their rights and obligations with respect to personal data protection. This encompasses the provision of unambiguous information regarding the practices of data collection, processing, and storage, as well as the repercussions of data breaches.

Execute technical measures: Enforce data security through the implementation of robust technical measures, including encryption, secure data storage, and regular software updates. Development and utilization of digital infrastructure that facilitates secure data transfer and processing are included in this.

Ensure Compliance with Data Protection Regulations: Implement effective enforcement mechanisms to guarantee adherence to data protection regulations. This entails the establishment of specialized agencies, such as the Department of Cybersecurity and Hi-tech Crime Prevention within the Ministry of Public Security, to address data protection violations and offer guidance on compliance.

Encourage Digital Governance: By utilizing digital platforms to optimize government operations, increase transparency, and improve citizen engagement, digital governance can be promoted. This encompasses the

integration of data protection into government-citizen interfaces and the guarantee that government agencies implement data protection in their own operations.

Promote Data-Driven Innovation: By offering businesses incentives to invest in data analytics and digital technologies, we can encourage data-driven innovation. This encompasses the provision of tax exemptions, subsidies, or other forms of assistance to encourage the expansion of the IT sector in Vietnam.

Monitor and Assess Progress: Assess the efficacy of data protection measures on a regular basis, taking into account both their successes and their persistent challenges. This involves executing regular evaluations and assessments to identify areas for improvement and to guarantee that data protection practices are consistent with the changing digital trends and technologies.

Vietnam can guarantee the security and sustainability of its digital transformation by achieving a balance between data protection and digital innovation through the implementation of these strategies.

CONCLUSION

The rapid digitalization of Vietnam has resulted in an urgent requirement for strong measures to protect personal data online. This study has emphasized the challenges and potential that come with the nation's digital expansion, underscoring the significance of a thorough regulatory framework, improved awareness among the public, and improved policing procedures. Vietnam can establish a strong digital ecosystem that integrates economic expansion with personal privacy and security by tackling these challenges and benefiting on these advantages.

This study's results emphasize the importance of an integrated approach for protecting personal data online, which should involve collaboration between government and private sector entities. Implementing a comprehensive legal framework, along with conducting extensive public awareness campaigns and strengthening enforcement mechanisms, can effectively safeguard personal data in Vietnam.

The ultimate success of Vietnam's digital transformation depends on its capacity to achieve an acceptable balance between economic growth and the protection of individual privacy and security. By giving high importance to defending online personal data, the country can establish a strong and secure digital environment that promotes both economic growth and personal rights.

Statements and Declarations

Conflicts of Interest: The authors report there are no competing interests to declare.

Funding: The authors received no specific funding for this work.

Ethical Approval: This article does not contain any studies with human participants performed by any of the authors.

Informed Consent: This article does not contain any studies with human participants performed by any of the authors.

REFERENCES

Cameron, Pham TH, Atherton J, et al (2019) Vietnam's future digital economy - Towards 2030 and 2045. In: Commonw. Sci. Ind. Res. Organ. https://research.csiro.au/aus4innovation/foresight/. Accessed 20 Feb 2022

Civil Code and the Law on Cyberinformation Security and Law on Electronic Transactions and the Law on Telecommunications Vietnam - Data Protection Overview

IPS & UNDP Vietnam (2022) Review of Local Governments' Implementation of Personal Data Protection on Online Government-Citizen Interaction Interfaces. Policy Studies and Media Development (IPS) and UNDP Vietnam

National Assembly of the Socialist Republic of Vietnam (2018) Law on Cyber Security No. 22/2018/QH14

Open Development Vietnam (2023) Vietnam Digital Transformation Agenda. Open Development Vietnam

Statista Market Insights (2024) Digital & Connectivity Indicators - Vietnam | Forecast. Statista

United Nations in Viet Nam (2023) How the UN is supporting The Sustainable Development Goals in Viet Nam

Vietnam Government (2023) Decree 13/2023/ND-CP on the protection of personal data issued by the Government. Vietnam Government, Hanoi.