

HO CHI MINH NATIONAL ACADEMY OF POLITICS

CAO NGUYEN HUNG

**PROTECTION OF PERSONAL DATA RIGHTS IN THE CONSTRUCTION
OF PROVINCIAL-LEVEL DIGITAL GOVERNMENT IN VIETNAM**

**SUMMARY OF PH.D. THESIS
MAJOR: HUMAN RIGHTS LAW
CODE: PILOT TRAINING**

HA NOI - 2026

**THE THESIS WAS COMPLETED AT
HO CHI MINH NATIONAL ACADEMY OF POLITICS**

SCIENTIFIC SUPERVISORS:

1. Assoc. Prof. Dr. Vu Trong Lam



2. Dr. Tran Thị Hong Hanh



Reviewer 1:

.....

Reviewer 2:

.....

Reviewer 3:

.....

**The thesis will be defended before the Thesis Examination Council meeting
at the Ho Chi Minh National Academy of Politics**

at hours on day month year

The thesis can be found at:

- National Library of Vietnam

- Library of the Ho Chi Minh National Academy of Politics

HANOI - 2026

INTRODUCTION

1. Urgency of the Topic

The research and selection of the topic: *"Protection of Personal Data Rights in the Construction of Provincial-Level Digital Government in Vietnam"* at the Ph.D. level majoring in Human Rights Law is a vital requirement, stemming from the following fundamental reasons:

First, amidst the profound development of the Fourth Industrial Revolution, data in general, and personal data (PD) in particular, has become a vital resource playing a foundational role in socio-economic development, national governance innovation, and digital government construction. In Vietnam, the Party and State have identified national digital transformation, the building of a digital Government, and digital governance as core tasks with long-term strategic significance, especially for the 2026–2030 period. Localities, particularly provincial-level digital governments, play an exceptionally crucial role in Vietnam's state governance system and are robustly deploying shared databases, data centers, digital platforms, and data-sharing systems to serve state management.

Second, the scale and intensity of personal data processing are increasing rapidly, whereas data governance capacity, human resources, technical conditions, and control mechanisms in many localities remain constrained. This escalates the risk of violations against personal data rights and necessitates an urgent need to perfect the theoretical foundation, legal framework, and enforcement mechanisms for protecting personal data rights in the establishment of provincial-level digital governments.

Third, protecting personal data rights is an intrinsic requirement of the Socialist Rule-of-Law State of Vietnam, where human rights (HR) and citizen rights (CR) are respected, protected, and guaranteed under the Constitution and laws. Vietnam is accelerating digital transformation and perfecting the legal corridor on data rights to deeply integrate into new-generation free trade agreements and international cooperation; hence, standardizing data protection procedures according to stringent standards is imperative. Accordingly, numerous legal documents have been promulgated to protect personal information and ensure data security in the digital environment. Notably, the National Assembly's passage of the Personal Data Protection Law (taking effect on January 1, 2026) marks a significant milestone in perfecting the legal system on human rights in the digital environment in Vietnam.

Fourth, from the perspective of legal science, although several studies exist on personal data, personal data protection, privacy, e-government, or digital government, in-depth and systematic research on protecting personal data rights in provincial-level digital government construction in Vietnam remains relatively scarce. Specifically, few studies approach this issue from a human rights perspective, tied to the requirements of building a socialist rule-of-law state,

implementing national digital transformation, and deploying the Personal Data Protection Law within local government practices-particularly regarding personal data rights protection in provincial-level digital governments today. This gap highlights the theoretical and practical significance of the topic.

2. Objectives and Research Tasks of the Topic

2.1. Research Objectives

Based on researching theoretical and practical issues regarding the protection of personal data rights in the construction of provincial-level digital governments in Vietnam, the thesis thoroughly analyzes and evaluates the current state of personal data rights protection to contribute to theoretical enrichment; subsequently proposing effective solutions to protect personal data rights in Vietnam's provincial-level digital governments today, ensuring a balance between technological governance development goals and the respect, protection, and promotion of human rights and citizen rights.

2.2. Research Tasks

One, conduct a literature review of scientific works related to personal data rights protection in provincial digital government construction globally and domestically, evaluating existing research while identifying gaps for further investigation.

Two, research and clarify the fundamental theoretical basis of personal data rights in digital government construction, including: concepts, characteristics, roles, contents, modalities, influencing factors, international law, comparative foreign laws, and valuable lessons for Vietnam; along with its relationship with privacy and human rights in the digital transformation context.

Three, research, analyze, and evaluate the status quo of law and practice in personal data protection during the establishment of provincial digital governments in Vietnam, thereby identifying inadequacies, limitations, and their root causes.

Four, propose perspectives, solutions, and policy recommendations to perfect legislation and enhance enforcement capacity for better personal data rights protection in provincial digital government construction in Vietnam today.

3. Subject and Scope of Research

3.1. Subject of Research

The subject of research comprises social relations, theoretical perspectives, legal provisions, and law enforcement practices regarding personal data rights protection in the process of building provincial-level digital governments in Vietnam. Specifically:

From a theoretical standpoint: Researching academic viewpoints and legal ideologies on personal data rights under the lens of human rights and citizen rights; the connotations, characteristics, principles, and criteria for guaranteeing these rights within local public governance environments.

From a legal-institutional standpoint: Examining current Vietnamese legal provisions, focusing on Decree No. 13/2023/NĐ-CP, the Personal Data Protection Law (Law No. 91/2026/QH15), implementing guiding documents, and regulations governing provincial digital government structures.

From a practical standpoint: Investigating law enforcement practices, barriers, conflicts of interest, violations, and operational inadequacies within current provincial digital government systems from a human rights protection perspective.

3.2. Scope of Research

Content scope: The thesis focuses on examining the protection of personal data rights during the deployment of provincial digital governments, based on international and Vietnamese legal frameworks. It centers on personal data rights protection within the legal relationship between Citizens (Rights-holders) and Provincial Local Governments (Duty-bearers).

Spatial scope: Restricted to personal data rights protection in provincial digital government construction in Vietnam, analyzing national-level policies while deeply evaluating implementation practices across representative localities.

Temporal scope: Concentrating on law enforcement practices from 2020 to 2025 and the first half of 2026.

4. Theoretical Basis and Research Methods

4.1. Theoretical Basis The thesis is grounded in Marxist-Leninist dialectical materialism and historical materialism, Ho Chi Minh Thought, and the viewpoints of the Party and State on human rights and citizen rights.

4.2. Research Methods

The thesis employs literature review as the foundation for the entire research process, alongside methods including: analysis-statistics-synthesis; comparison; expert and managerial interviews/consultations; systematization-logic and induction; case studies; and dialectical methodology applied to examine personal data rights protection in the interactive relationship between digital government development and human rights/citizen rights protection.

5. New Contributions of the Topic

First, the thesis contributes to systemizing and clarifying the theoretical foundation for personal data rights protection in the context of provincial digital government construction, elucidating core concepts, principles, substantive rights contents, and protection modalities amid data interoperability, administrative procedure digitalization, and online public service delivery.

Second, the thesis constructs and develops a multi-layered legal-governance analytical framework to evaluate personal data rights protection effectiveness in provincial digital governments, encompassing: international human rights and privacy law; national legislation and institutional frameworks on personal data protection and public sector data governance; and the

local operational tier linked to organizational structures, operational workflows, and digital technical infrastructure. It clarifies the relationship between data subjects' rights and data processing entities' obligations, emphasizing accountability, transparency, and the control of data power in the public sector.

Third, the thesis conducts selective comparative research on international legal standards and models from Germany, the Russian Federation, China, Singapore, and Thailand, extracting valuable reference lessons for Vietnam.

Fourth, based on evaluating provincial-level realities, the thesis identifies specific limitations and challenges, focusing on: risks of repurposed data exceeding authorized objectives during interoperability; lack of transparency towards data subjects; shortcomings in rights enforcement mechanisms (access, rectification, restriction of processing, objection, withdrawal of consent); inadequacies in audit trailing and burden of proof; and weaknesses in sanction deterrence and legal redress. Consequently, it provides scientific arguments for perfecting provincial digital government protection mechanisms, serving policymaking, operational rule-making, and local capacity-building.

6. Theoretical and Practical Significance

6.1. Theoretical Significance: A comprehensive, in-depth research work providing novel knowledge, arguments, and proposals of high reference value for promoting personal data rights in Vietnam.

6.2. Practical Significance: Serves as reference material for teaching and researching human rights specialization at the Institute for Human Rights, Ho Chi Minh National Academy of Politics, and other training institutions nationwide.

7. Thesis Structure

Aside from the Introduction, Conclusion, References, and Appendices, the thesis comprises 4 chapters:

Chapter 1: Literature Review on Research Related to the Topic

Chapter 2: Theoretical Basis for Protecting Personal Data Rights in Provincial-Level Digital Government Construction

Chapter 3: Current Status of Personal Data Rights Protection in Provincial-Level Digital Government Construction in Vietnam

Chapter 4: Perspectives and Solutions for Protecting Personal Data Rights in Provincial-Level Digital Government Construction in Vietnam Today

CHAPTER 1

LITERATURE REVIEW

1.1. Domestic Research Related to the Thesis Topic1.

1.1. Research Works on E-Government and Digital Government in the Context of National Digital Transformation

Existing research works have approached relatively comprehensively the issues regarding concepts, characteristics, roles, models, and solutions for building e-governments, digital governments, and digital administrations in Vietnam. However, these studies primarily focus on governance dimensions, organizational structures, technological infrastructure, and administrative reform. Meanwhile, the protection of personal data rights during the construction of digital governments-particularly at the provincial level-has only been addressed indirectly and has not yet become the object of in-depth legal research. This constitutes the research gap that the thesis aims to clarify.

1.1.2. Research Works on Personal Data Protection and Personal Data Rights Protection in Digital Government Construction

1.1.2.1. Research Works on Personal Data Protection in Digital Government Construction

Research works such as dissertations, monographs, reference books, and scientific workshop proceedings generally approach personal data protection from a general dimension or through legal comparison. They have not yet systematically clarified the issue of protecting personal data rights during the construction and operation of digital governments, particularly at the provincial level. This constitutes the research gap that the thesis focuses on clarifying.

1.1.2.2. Research Works on Personal Data Rights Protection in Digital Government Construction

Domestic research works, monographs, reference books, and textbooks play an important role in shaping the theoretical foundation for research on personal data rights protection, especially when placed in the context of digital government construction. However, considered strictly within the framework of researching personal data rights protection in the construction and operation of digital governments, there remains a requirement for continued systematization within the space of public governance.

1.2. Foreign Research Related to the Thesis Topic

1.2.1. Foreign Research Works on E-Government and Digital Government

International research has contributed an important academic foundation for explaining the nature, characteristics, and developmental requirements of digital governments in the context of global digital transformation. Nevertheless, limitations remain, including a shortage of systematic quantitative and qualitative research on citizens' satisfaction levels and interaction, as well as an inadequate discussion of the risks, challenges, and threats of human rights violations in the digital environment. This represents the scientific gap that the thesis aims to clarify within the context of current provincial-level digital government construction in Vietnam.

1.2.2. Foreign Research Works on Personal Data Protection and Personal Data Rights Protection in Digital Government Construction

1.2.2.1. Foreign Research Works on Personal Data Protection

These research works approach the subject through primary orientations, ranging from the theoretical foundation of privacy rights to the establishment of international legal standards, regional legal models, and data governance within the public sector and digital government. However, translating these research findings into the context of digital government construction and operation in individual countries, particularly at the local level, still poses a requirement for ongoing research to ensure appropriateness and effectiveness in protecting personal data rights.

1.2.2.2. Research Works on Personal Data Rights Protection in Digital Government Construction

These research works approach the subject not only from the technical perspective of public sector digitalization but also expand into data governance, state accountability, human rights protection in cyberspace, and the control of risks arising from emerging technologies.

1.3. Issues to be Further Researched by the Thesis

1.3.1. General Evaluation of Previous Research Works and Academic Gaps

Domestic and international research works related to personal data protection and digital government have laid an important foundation; however, under the lens of scientific critique, these studies still exhibit theoretical limitations and leave core academic gaps: (1) A shortage of theoretical foundations regarding the "rights enforcement guarantee mechanism" in the public sector; (2) A gap regarding a dedicated "theoretical model and guarantee mechanism framework" tailored for local government levels; (3) Fragmentation among legal, organizational, and technical protection modalities.

Solutions and New Contributions of the Thesis: These very theoretical gaps concerning the aforementioned "rights enforcement guarantee mechanism" constitute the room and primary objective that the thesis focuses on resolving: (1) Constructing a comprehensive theoretical framework on the guarantee mechanism for personal data rights in provincial-level digital governments, through a system of data power control principles and synchronized protection modalities; (2) Comprehensively evaluating and testing the status quo of rulemaking and enforcement at the local level, thereby proposing synchronized models and solutions with high feasibility in contemporary Vietnam.

1.3.2. Contents to be Further Researched by the Thesis

(1) Constructing a comprehensive theoretical framework on the guarantee mechanism for personal data rights in provincial-level digital governments; (2) Conducting a comparative analysis of international legislative experiences and implementation models; (3) Examining the status quo of rulemaking and enforcement concerning personal data rights protection in provincial-level

digital governments in Vietnam; (4) Proposing a system of synchronized solutions and a feasible rights enforcement guarantee model in Vietnam.

1.4. Research Hypothesis and Research Questions

1.4.1. Research Hypothesis

The research hypothesis of the thesis posits that: The current effectiveness of personal data rights protection in provincial-level digital government construction is constrained not due to pure technical-technological barriers, but stems from institutional gaps and administrative management mindsets; specifically, the deficiency in public power control mechanisms during data processing and citizens' passivity in digital self-defense. Therefore, the effectiveness of personal data rights protection in provincial-level digital governments can only be achieved substantively and sustainably through a shift from an administrative management mindset to a human rights-based approach, via three core legal pillars: regarding State agencies; regarding citizens; and regarding guarantee mechanisms.

1.4.2. Research Questions

The thesis focuses on addressing questions regarding: The theoretical foundation and international/national legal standards on personal data rights protection under a human rights lens in the construction of provincial-level digital governments in Vietnam; contents and modalities; the current status, limitations, and causes in enforcing personal data rights protection in provincial digital governments. Simultaneously, it identifies breakthrough solutions for protecting personal data rights in Vietnam in the ensuing period.

CHAPTER 2

THEORETICAL BASIS FOR PROTECTING PERSONAL DATA RIGHTS IN PROVINCIAL-LEVEL DIGITAL GOVERNMENT CONSTRUCTION

2.1. Concepts, Characteristics, and Roles of Personal Data Rights Protection in Provincial-Level Digital Government Construction

2.1.1. Concept of Personal Data Rights Protection in Provincial-Level Digital Government Construction

2.1.1.1. Concept of Personal Data

"Personal data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

2.1.1.2. Concept of Personal Data Rights

Personal data rights are rights that emerge and develop strongly in the context of the digital society, and are generally perceived as a core component of the right to privacy—a fundamental human right that ensures the autonomy, dignity, and "personal space" of every individual.

2.1.1.3. Concept of Personal Data Rights Protection

Data Subject: An individual whose personal data is processed, pursuant to Clause 5, Article 2 of the 2025 Personal Data Protection Law. *Personal Data Rights Protection:* The totality of legal, technical, and organizational measures aimed at ensuring that individuals enjoy their rights regarding their personal data and preventing any unauthorized or unlawful infringement upon those rights.

Provincial-Level Local Government: A key intermediate tier that both represents local citizens and exercises the executive power of the State within a specific territorial jurisdiction.

2.1.1.4. Concepts of Digital Government and Provincial-Level Digital Government

"Digital Government" is a model of government operating primarily based on the application of digital technology to continuously innovate governance methods, thereby enhancing the efficacy and efficiency of state apparatus operations. "Provincial-level digital government" is the model of local government at the provincial level in which provincial-level governmental organs—with the People's Council and the People's Committee as the core—organize operations and execute their tasks and powers primarily within a digital environment. This model relies on digital infrastructure, digital platforms, digital data, and digital technology applications to improve governance processes, enhance data-driven administrative capacity, elevate the quality of public service delivery, ensure transparency and interactivity with citizens and enterprises, thereby enhancing the efficacy and efficiency of state management at the provincial scope.

2.1.1.5. Concept of Personal Data Rights Protection in Provincial-Level Digital Government Construction

This is a comprehensive composite process that requires the synchronized combination of legal regulations, implementation organization, technical solutions, and rights-guarantee mechanisms for data subjects, aiming toward the goal of developing a human-centric digital government while ensuring effective state governance in the digital environment.

2.1.1.6. Distinguishing Personal Data Rights from Related Concepts

To clearly distinguish personal data rights from related concepts such as: Personal data rights versus personal data protection; personal data protection versus information security and cybersecurity; and personal data protection versus data governance. Accordingly, personal data protection constitutes the mandatory legal boundary framework for public digital data governance.

2.1.2. Characteristics of Personal Data Rights Protection in Provincial-Level Digital Government Construction

2.1.2.1. Featuring a legal balance between the requirements of optimizing public governance and ensuring citizens' informational self-determination

This characteristic reflects the application of the principle of proportionality in controlling state power. Any intervention, collection, or sharing of personal data by provincial governments for public interest purposes is considered lawful only when it ensures necessity, minimization, and a legitimate purpose.

2.1.2.2. Entailing the resolution of "power asymmetry" between local governments and citizens in the digital environment

This characteristic stems from the nature of the legal relationship between the Rights-holder (Citizen) and the Duty-bearer (Provincial Government).

From the perspective of the Government: The integration and large-scale centralization of data at provincial specialized agencies create potential risks of over-surveillance or widespread data leakage.

From the perspective of Citizens: Citizens are typically in a vulnerable position, lacking legal interactive tools and facing barriers in digital literacy to exercise self-defense rights. Therefore, power balancing and safeguarding the position of citizens before public authorities are imperative.

2.1.2.3. Implemented through a multi-party mechanism for delineating legal liability and public accountability

Data rights protection in the provincial public sector is no longer a traditional unilateral relationship between the State and Citizens, but also involves technology enterprises (authorized third parties).

2.1.2.4. Ensuring the uniformity of national human rights standards while being governed by local enforcement peculiarities

This is a manifestation of the relationship between institutional uniformity (the Constitution, laws, and international treaties) and flexibility in local governance; provincial levels must materialize implementation procedures to be both suitable to local conditions and steadfast in upholding national human rights protection standards.

2.1.3. Roles of Personal Data Rights Protection in Provincial-Level Digital Government Construction

First, ensuring the constitutionality and legality of data governance activities in the public sector. *Second*, serving as the basis for establishing and maintaining digital trust between provincial governments and citizens/businesses. *Third*, contributing to improving the quality of state management and the efficiency of public service delivery. *Fourth*, serving as an inevitable requirement in international integration and local economic development. *Fifth*, acting as a crucial

factor in preventing and mitigating risks, cyber law violations, information security breaches, and operational risks within provincial digital government systems.

2.2. Contents, Modalities, and Influencing Factors of Personal Data Rights Protection in Provincial-Level Digital Government Construction

2.2.1. Contents of Rights and Contents of Personal Data Rights Protection in Provincial-Level Digital Government Construction

2.2.1.1. Contents of Citizens' Personal Data Rights in Provincial-Level Digital Government Construction

Citizens' personal data rights in relation to the provincial digital government comprise a bundle of legal entitlements falling under Informational Self-Determination. In the provincial digital government environment, this system of rights is constituted by 03 core rights groups: (1) The group of information access and processing rights; (2) The group of intervention and digital intervention rights; (3) The group of self-defense and legal support rights.

2.2.1.2. Contents of Personal Data Rights Protection by Provincial Digital Governments

Personal data rights protection is the process by which provincial digital governments fulfill national human rights obligations through citizens' 6 rights groups via the following primary pillars: (1) Ensuring minimum legal principles in data processing; (2) Clearly delineating the legal liabilities of subjects participating in data relations; (3) Implementing technical security, safety, and internal governance measures; (4) Resolving the dialectical relationship between "Data Interoperability and Sharing" and "Security and Privacy Control"; (5) Operating control, inspection, auditing mechanisms, and enhancing enforcement capacity.

2.2.2. Modalities of Personal Data Rights Protection in Provincial-Level Digital Government Construction

2.2.2.1. Modality of policy formulation and perfecting local laws on personal data rights protection

Theoretically, this modality is constituted by three core connotations: *First*, localizing central legal standards into the regional governance context; *Second*, synchronizing technical-technological workflows with legal norms; *Third*, establishing liability institutions and remedies for restoring rights.

2.2.2.2. Modality of organizational restructuring and establishing internal management mechanisms for personal data rights protection in provincial digital governments

First, modeling subject roles and delineating legal liabilities according to substantive power. *Second*, establishing specialized organizational structures and individualizing administrative responsibilities. *Third*, proceduralizing minimal authority and closed-loop official audit trails.

2.2.2.3. Modality of employing modern technical infrastructure, technology, and data governance measures

This modality is constituted by four foundational technical pillars: *First*, multi-state data encryption under risk-isolation principles; *Second*, access control mechanisms based on the "Least Privilege" principle and Zero Trust philosophy; *Third*, automated monitoring and logging technologies creating immutable evidence; *Fourth*, anonymization techniques in smart data lifecycle management.

2.2.2.4. Modality of implementing inspection, auditing, violation handling, and damage compensation mechanisms

Theoretically, this modality operates based on 03 mechanisms: *First*, official inspection and auditing mechanisms based on mandatory accountability principles; *Second*, a tiered system of deterrent sanctions; *Third*, perfecting comprehensive damage compensation and rights-restoration mechanisms.

2.2.2.5. Modality of communication and education to raise public awareness and digital literacy regarding personal data protection

Communication and education serve as proactive protection modalities through two components: *First*, establishing digital literacy and self-protection mechanisms for data subjects (Citizens); *Second*, shaping a culture of compliance and data professional ethics in the public sector.

2.2.2.6. Modality of international cooperation and controlled information sharing

This modality operates via 03 connotations: *First*, internalizing universal global legal and technological standards; *Second*, establishing legal filters and power decentralization within data-sharing mechanisms; *Third*, multi-layered coordination mechanisms and rapid response to cross-border security risks.

2.2.3. Influencing Factors on Personal Data Rights Protection in Provincial-Level Digital Government Construction

2.2.3.1. Personal data rights protection must be placed within the framework of Party leadership and socialist rule-of-law state orientation

The viewpoints and guidelines of the Communist Party of Vietnam serve as the core political-theoretical foundation guiding the shift in governance mindset for provincial digital government construction.

2.2.3.2. Characteristics of public administrative governance and policy (regulation) translation capacity of provincial government machinery

Unlike national legal norms which possess an instrumental protective nature, the administrative governance capacity and policy-materialization skills of the provincial apparatus are practical factors directly impacting local rights protection efficacy: (1) Administrative latency and implementation rule-making capacity; (2) Official psychology and responsibility boundary demarcation; (3) Compatibility and convergence with international governance standards (such as the GDPR).

2.2.3.3. Development level of technological infrastructure and data security solutions

(1) Synchronicity and standardization of local digital infrastructure; (2) Presence of core technical protection solutions; (3) Challenges from emerging technologies (AI, Big Data).

2.2.3.4. Professional proficiency, digital literacy, and public service ethics of cadres and civil servants

Humans act as both system operators and subjects: (1) Digital literacy and information security skills; (2) Public service ethics and administrative discipline; (3) Workplace culture and accountability awareness.

2.2.3.5. Financial resources and public investment for information security:

(1) Budget allocation ratio for information security; (2) Capability to maintain and upgrade systems.

2.2.3.6. Citizens' legal awareness, digital literacy, and social monitoring/criticism mechanisms

(1) Legal awareness and digital self-defense capacity of data subjects (Citizens); (2) Enforcement channels and compliance costs; (3) Oversight by elected bodies, media, and partner enterprises.

2.3. International Law and Practices of Selected Countries Regarding Personal Data Rights Protection in Digital Government Construction

2.3.1. International Law on Personal Data Rights Protection

Within international human rights law, personal data rights protection is formed and developed on the foundation of the right to privacy, which is recognized as a fundamental and universal right. Contents and modalities include: (1) Protection via the principle of "Data Minimization and Purpose Limitation"; (2) Protection via "Transparency and the Right to Know"; (3) Protection via "Informational Self-Determination and Consent"; (4) Protection via "Deep Intervention in the Data Lifecycle"; (5) Protection via "Privacy by Design and by Default"; (6) Protection via "Cross-Border Data Flow Control"; (7) Protection via "Jurisdiction, Litigation, and Damage Compensation" sanctions.

2.3.2. Typical National Laws on Personal Data Rights Protection in Digital Government Construction

2.3.2.1. Delineating the legal value of relevant international and regional normative sources

Global legally binding international conventions (such as the ICCPR): Establish supreme international legal obligations regarding human rights and privacy.

Specialized international treaties (such as Convention 108 and Amending Protocol 108+ of the Council of Europe): The first legally binding multilateral international convention on data protection, open to non-European nations.

Regional laws (such as the EU GDPR): Model legislation with direct effect and legal binding force across EU member states.

Governance standards and soft guidelines (such as OECD Recommendations): Non-coercive legally, yet shaping good governance principles.

2.3.2.2. Survey of legal models and Central-Local power structures of typical countries regarding personal data rights protection in digital government construction

(1) Federal Republic of Germany: Federal model, constitutional jurisprudence, and the GDPR-BDSG integration. In digital government construction, Germany closely aligns with the Online Access Act (OZG and OZG 2.0), viewing data protection as a constitutive condition for connecting interoperable public service portals across government tiers.

(2) China: Centralized power model and the "Trinity" of national security data laws: the Personal Information Protection Law (PIPL) combined with the Cybersecurity Law (CSL) and Data Security Law (DSL). PIPL features a dedicated chapter regulating state agencies' obligations when processing data for statutory tasks. (iii) Monitoring and sanctioning mechanisms: The Cyberspace Administration of China (CAC) coordinates globally. Penalties are extremely severe (administrative fines up to 50 million RMB or 5% of annual turnover for serious violations).

(3) Russian Federation: Federal model, data localization, and inter-agency interoperability; combining federal power with federal subjects. Privacy rights are constitutionally and federally enshrined. Public service provision and inter-agency data sharing occur through the Interdepartmental Electronic Interaction System. The specialized supervisory body Roskomnadzor conducts compliance inspections.

(4) Singapore: Smart Nation model, public-private segregation, and normative convergence. The 2012 PDPA regulates the private sector, while the public sector is governed by the Electronic Government Act and Government Data Office directives; core data subject rights principles apply relatively strictly across both sectors. The PDPC coordinates generally and enforces heavy financial penalties (up to 10% of turnover or 1 million Singapore dollars).

(5) Thailand: Public-private consolidated legislative model and GDPR internalization in Southeast Asia: Thailand's Personal Data Protection Act (PDPA 2019) is designed as a consolidated law applied comprehensively and uniformly to both the private sector and state agencies, including local administrations and provincial governors. Operationally regarded as a successful regional "internalization" of the GDPR, the Act grants citizens robust rights (access, rectification, objection, right to be forgotten). The independent PDPC adjudicates enforcement; local administrative agencies are mandated to appoint a DPO and conduct Data Protection Impact Assessments (DPIA). Administrative fines reach up to 5 million Baht, alongside civil compensation liabilities (double actual damages) and criminal penalties (imprisonment up to 1 year).

2.3.3. Lessons Learned for Personal Data Rights Protection in Provincial-Level Digital Government Construction in Vietnam

Lessons for Vietnam include ensuring compatibility and synchronization between the PDP Law and specialized laws (Archives Law, Land Law, Identification Law). Locally, provincial governments must proactively issue internal regulations and Standard Operating Procedures (SOPs) to materialize central directives to fit local managerial practices. International jurisdictions mandate that data-processing entities appoint specialized Data Protection Officers (DPOs) and maintain rigorous internal governance documentation. Provincial tiers in Vietnam must explicitly institutionalize independent DPO models within specialized organs under provincial People's Committees. Data protection transcends administrative documents; it must be coded into technical infrastructure to operationalize secure yet controllable data interoperability. Furthermore, enhancing the authority of specialized data protection agencies and sustaining regular specialized inspections (such as Germany's BfDI, Russia's Roskomnadzor, or Thailand/Singapore's PDPC) backed by rigorous sanctions is vital.

In summary, international models consistently position personal data rights as the materialization of privacy and informational self-determination, placing humans at the center of all digital government development strategies.

Chapter 2 Summary

Chapter 2 has established the theoretical foundation for researching personal data rights protection in provincial digital government construction; outlined provincial-level data protection characteristics linked to contexts where data is processed primarily for administrative procedures and online public services, alongside frequent inter-agency coordination and data interoperability. Regarding contents and protection modalities, the thesis systematized data subjects' rights groups and requirements for ensuring rights enforceability in the digital environment; obligations of data processing entities; and enforcement guarantee mechanisms. It analyzed influencing factors on data rights protection efficacy and examined international legal standards and foreign practices to derive valuable reference suggestions for Vietnam.

CHAPTER 3

CURRENT STATUS OF PERSONAL DATA RIGHTS PROTECTION IN PROVINCIAL-LEVEL DIGITAL GOVERNMENT CONSTRUCTION IN VIETNAM

3.1. General Overview of the Current Status and Influencing Factors on Provincial-Level Digital Government Construction Regarding Personal Data

3.1.1. Guidelines and Policies of the Party and State on Developing Provincial-Level Digital Government in Vietnam Today

Provincial-level digital government is an organic component that determines the success or failure of the national digital transformation strategy. The system of guidelines and policies of the

Party and State on this issue is consistent, promoting the simultaneous advancement of both digital productive forces and digital production relations at the local level. It adopts a people-centric approach; treats data as a resource; and links development with information security and the protection of citizens' data confidentiality rights.

3.1.2. Current Status of Provincial-Level Digital Government Construction in Vietnam

The scale and sensitive nature of personal data within provincial governments over recent years represent both a major achievement of digital transformation and an enormous source of legal risks regarding human rights. While helping provincial governments streamline their administrative machinery, make data-driven governance decisions, and deliver ultra-fast public services, data repositories containing the entire private lives of millions of citizens also become targets for cyberattacks or are easily compromised due to carelessness and the abuse of lookup rights by grassroots-level cadres and civil servants. Consequently, robust modalities for protecting personal data rights at the local level are imperative.

3.1.3. Identifying Risks and Challenges to Personal Data Rights in the Provincial Digital Environment

Through research on digital administrative implementation practices, the risks and challenges to personal data rights in the provincial digital environment are evident. While provincial governments are empowered to maximize data collection to serve administrative management and economic development goals, the legal tools available for citizens to exercise self-defense rights in practice remain extremely weak and formalistic. This constitutes the most profound structural bottleneck that must be resolved through breakthrough solutions in guarantee institutions.

3.2. Current Status of Deploying Contents and Modalities for Personal Data Rights Protection in Provincial-Level Digital Government Construction in Vietnam

3.2.1. Current Status of Legal Regulations on Personal Data Rights Protection in Provincial-Level Digital Government Construction in Vietnam

3.2.1.1. Current Status of Regulations on the Contents of Personal Data Rights

Personal data rights are gradually being recognized as a constituent component of human rights, linked to the right to privacy, the inviolability of personal life, and the right to the protection of individual human dignity and honor. From the perspective of human rights theory, personal data rights not only signify the protection of individuals against arbitrary interference by the State and other entities, but also reflect the requirement to empower individuals with the capability to control information about themselves within a digitized environment (expressed through 6 groups of rights).

3.2.1.2. Current Status of Regulations on Subjects Responsible for Protecting Personal Data Rights in Provincial-Level Digital Government Construction in Vietnam

Over recent years, although numerous regulatory instruments have been promulgated, institutional modalities and internal regulations at the provincial level still exhibit major bottlenecks, including: (1) Formality and "verbatim copying" of higher-level documents; (2) Internal regulations failing to keep pace with new smart city technologies; (3) Laxity in binding contractual rules with technology contractors (third parties). The absence of strict technical and legal regulations to monitor and penalize enterprises creates risks of citizens' data being covertly appropriated by contractors.

3.2.1.3. Current Status of Personal Data Collection and Processing via Provincial Platforms and Public Service Portals

The practice of personal data processing on provincial public service platforms reveals escalating risks of cyberattacks and data theft, severely infringing upon personal data and the data rights of data subjects in the contemporary period. A 2025 cybersecurity survey report indicates that information systems in Vietnam faced approximately 552,000 cyberattacks, with 52.30% of agencies and enterprises continuing to record losses resulting from cyberattacks.

3.2.2. Current Status of Organizational Structure, Personnel Management, and Responsibility Demarcation for Personal Data Rights Protection in Provincial Agencies

During the implementation of provincial digital governments in the 2020–2025 period, the majority of specialized agencies under provincial People's Committees have formed units related to information system operations, digital transformation, administrative procedure control, or administrative reform. Nevertheless, practical implementation demonstrates that the modality of protecting personal data rights through local organizational structures remains in a "running while lining up" phase, revealing numerous inadequacies in both structural design and operational capacity. This reality manifests clearly across three structural dimensions: (i) Focal point organization; (ii) Responsibility demarcation along the data processing chain; (iii) Coordination mechanisms for handling data subjects' requests and incident response.

3.2.3. Current Status of Technical Infrastructure and Technologies Ensuring Cybersecurity to Protect Personal Data Rights in Provincial-Level Digital Government Construction

Technical infrastructure and cybersecurity technologies for administrative information systems have achieved significant progress in both investment scale and coverage. However, viewed from the perspective of personal data rights protection, this reality exposes a stark discrepancy between the expansion of data processing systems and corresponding data protection capabilities, particularly at the local level—the direct operator of public service portals, administrative procedure resolution systems, and specialized databases. The risk of data leakage

caused by Cloud security flaws impacts human rights; this directly violates citizens' data safety and privacy rights, exposing them to risks of threats, fraud, or defamation. This reality reflects deficiencies in public authorities' compliance with safety standards. When incidents occur, if governments lack instant warning mechanisms for citizens and fail to establish damage compensation liabilities, the rights protection mechanism fractures.

3.2.4. Current Status of Inspection, Auditing, Complaint Resolution, and Violation Handling Regarding Personal Data Rights Protection in Provincial-Level Digital Government Construction

Inspection, auditing, complaint and denunciation resolution, and violation handling play a pivotal role in ensuring the right to protection and effective redress when personal data is violated. However, implementation practices show that control and sanctioning capacities in this domain have yet to keep pace with the expansion of digital governments, especially at the provincial level—where the vast majority of data processing activities directly originate.

3.2.5. Current Status of Communication, Dissemination, and Awareness Raising for Cadres, Civil Servants, Citizens, and Society Regarding Personal Data Rights Protection in Provincial-Level Digital Government Construction

Communication modalities across provinces in recent times show that while results have been achieved, depth and "substance" remain lacking. Citizens participate in digital governments in a "passive" stance, surrendering data because it is mandatory for resolving administrative procedures, without truly understanding how their data is protected, thereby suffering from a deficit of "digital trust."

3.2.6. Current Status of Contractual Execution and Legal Liability Binding Between Provincial People's Committees and Technology Corporations (Third Parties) in Procuring Cloud Infrastructure or Public Administration Software Solutions

Amid limited internal budgets and technical human resources, local governments predominantly select "IT Service Outsourcing" models or strategic partnerships with major technology corporations such as VNPT, Viettel, and FPT to build cloud infrastructures, public service portals, and Smart Operation Centers (IOCs). While accelerating local digital transformation, this cooperative modality poses unprecedented challenges in controlling interoperability, data sharing, and safeguarding citizens' personal data rights against third parties.

3.3. Evaluation of the Current Status of Personal Data Rights Protection in Provincial-Level Digital Government Construction

3.3.1. Achievements in Personal Data Rights Protection in Provincial-Level Digital Government Construction in Vietnam

3.3.1.1. Legislation on Personal Data Rights Protection in Provincial-Level Digital Government Construction Has Gradually Perfected and Aligned with Practical Operations in Vietnam

Personal data protection and information security are no longer secondary concerns; they have been institutionalized, integrated directly into provincial annual digital transformation plans, and established as mandatory scoring criteria for administrative reform and digital transformation indices.

3.3.1.2. Citizens' Rights to Access, Lookup, and Rectify Information Have Been Initially Implemented

Through the VNeID application, provincial governments have provided citizens with tools to proactively cross-check their own data. Upon discovering personal information discrepancies (regarding civil status, residence, land, etc.), the procedure for receiving and processing citizens' data rectification requests at "One-Stop-Shop" units operates swiftly and transparently in real time.

3.3.1.3. Upgrading Technical Infrastructure, Applying Technology, and Forming Multi-Layered Data Security Models Have Contributed to Protecting Personal Data Rights in Provincial-Level Digital Government Construction

The application and continuous updating of data security technologies have emerged as a prominent outcome, contributing significantly to personal data rights protection. Although modernization levels vary across localities, security technologies have been deployed regularly and updated according to emerging trends, establishing a crucial technical foundation for safeguarding personal data rights in digital government operations.

3.3.1.4. Awareness and Responsibility of Cadres and Citizens Regarding Personal Data Rights Protection Have Been Elevated

Information security, data confidentiality, and personal data protection contents have been integrated into training and professional development programs for cadres and civil servants at central and local levels, fostering a sense of responsibility in collecting, processing, and utilizing citizens' personal data during official duty execution.

3.3.1.5. Regarding Modalities for Ensuring Substantive Rights of Data Subjects

This represents the core modality aimed at transforming declaration-like legal provisions into practical utilities, empowering citizens to exercise their "data sovereignty" in relations with local public authorities.

3.3.1.6. Feedback and Violation Handling Activities Concerning Personal Data Rights in Provincial Digital Government Construction Have Been Deployed Swiftly and Promptly

State management agencies have intensified information security inspections, audits, and handling of personal data violations—particularly unauthorized collection, utilization, or commercialization of data. The detection and handling of several large-scale violations demonstrate

improved responsive capacities among functional agencies, enhancing deterrent efficacy and personal data rights protection.

3.3.1.7. Regarding Modalities of Cooperation and Data Flow Control for Personal Data Rights Protection in Provincial Digital Government Construction in Recent Times

Public-private partnerships through IT service outsourcing and cloud computing infrastructure are inevitable. Recently, provincial governments have made vital strides in mindset transformation-shifting from "blanket delegation" of systems to contractors to establishing sovereign control mechanisms over data flows, thereby protecting citizens' personal data rights against third-party access.

3.3.2. Causes of Achievements in Personal Data Rights Protection in Provincial-Level Digital Government Construction in Vietnam

Driven by the synchronized resonance between two groups of factors: technological engineering and institutional commands. This system of 7 modalities has functioned as a closed-loop mechanism, enabling local governments to effectively exploit digital resources for development while ensuring secure data sovereignty. Nevertheless, these causative success factors primarily address protection from the State's perspective.

3.3.3. Limitations and Causes of Limitations in Personal Data Rights Protection in Provincial-Level Digital Government Construction in Vietnam

3.3.3.1. Limitations in Personal Data Rights Protection in Provincial-Level Digital Government Construction in Vietnam

First, limitations in institutional, legal, and internal regulatory perfection. *Second*, limitations in organizational structure and personnel management. *Third*, limitations in applying technical and technological measures. *Fourth*, limitations in inspection, auditing, and violation handling. *Fifth*, limitations in protecting data subjects' substantive rights. *Sixth*, limitations in communication and public awareness-raising dissemination. *Seventh*, limitations in data flow cooperation and control.

3.3.3.2. Causes of Limitations in Personal Data Rights Protection in Provincial-Level Digital Government Construction in Vietnam

First, objective causes: (1) Inadequacies and legal conflicts originating at the central level; (2) The ultra-fast developmental pace of digital technology; (3) The anonymous nature of cross-border "black markets." *Second*, subjective causes: Institutional and internal regulatory gaps; organizational and personnel frameworks; technical and technological measures; inspection, auditing, and violation handling; guaranteeing citizens' substantive rights; communication and citizen awareness-raising; data flow cooperation and control.

Chapter 3 Summary

Citizens' data is being aggregated at ultra-high speeds via administrative commands, yet the legal and technical tools to protect citizens' legitimate rights operate at exceptionally low speeds. Digital governments must build "digital trust" among data subjects. This serves as the grounding to formulate orientations and solutions for enhancing personal data rights protection efficacy in provincial digital government construction in the subsequent chapter of the thesis.

CHAPTER 4

PERSPECTIVES AND SOLUTIONS FOR PROTECTING PERSONAL DATA RIGHTS IN PROVINCIAL-LEVEL DIGITAL GOVERNMENT CONSTRUCTION IN VIETNAM TODAY

4.1. Forecasting Context and Influencing Factors on Personal Data Rights Protection in Provincial-Level Digital Government Construction in the Period Ahead

4.1.1. Positive Influencing Factors

4.1.1.1. Resonance factor from the perfection and enforcement of the Personal Data Protection Law

The official entry into force of the Personal Data Protection Law creates a supreme and synchronized legal corridor; Government Decree No. 356/2025/NĐ-CP detailing the implementation of certain articles of the Personal Data Protection Law has completely dismantled overlapping bottlenecks with specialized laws. This serves as a solid legal framework for localities to materialize internal regulations.

4.1.1.2. Factors stemming from the perfection and absolute coverage of digital identity infrastructure (Project 06), electronic authentication (VNeID), and standardized shared data sharing

By early 2026, Project 06 completed its basic digitalization objectives with the coverage of VNeID electronic identity accounts reaching over 85% of adult citizens in Vietnam, deeply integrated into the administrative procedure resolution information systems of 34 provinces and cities. This synchronized development helps standardize the "source" data flow, minimizing citizens' burdens of submitting paper copies or repeatedly declaring raw data at One-Stop-Shop units.

4.1.1.3. Constantly enhanced cybersecurity capacity and standardized security governance within state agencies

Information security in localities has undergone a robust transformation from a "passive defense" model to a "4-layer proactive protection" model under the guidance of the Ministry of Science and Technology. The upward investment trend is clearly demonstrated by provinces completing the approval of security classification proposals for information systems (achieving a rate of over 90% for core systems by 2025).

4.1.1.4. Development of digital human resources and local data governance capacity

In digital government construction, localities have streamlined their apparatus toward establishing specialized positions dedicated to information security and personal data protection. Conducting training and issuing information security certificates for grassroots-level civil servants directly processing dossiers helps minimize risks of data leakage due to inadvertent errors.

4.1.1.5. Public-private partnerships and accessibility to modern data protection technologies

The trend of public-private partnerships in deploying digital government platforms is projected to continue rising due to the demand for shortening deployment timelines and leveraging enterprises' technological capabilities.

4.1.2. Negative Influencing Factors

In the coming years, provincial-level digital government construction will continue to accelerate as online public services expand, data is digitized and interoperable at deeper levels, and numerous governance decisions rely on data analytics and artificial intelligence applications. However, accompanying convenience and efficiency benefits are novel risks to human rights in the digital environment-particularly personal data rights-such as artificial intelligence; unauthorized data interoperability and repurposing; organizational and human resource capacities; supply chain risks; and widening gaps in security capabilities regarding personal data leakage in provincial digital government construction.

4.2. Perspectives on Protecting Personal Data Rights in Provincial-Level Digital Government Construction in Vietnam

4.2.1. Personal data rights protection must be a core principle in guaranteeing human rights and citizen rights in the digital environment

All provincial-level policies and technological applications must be human-centric; radically shifting from the mindset of "managing data to serve official duties" to the mindset of "governing data to protect citizens' legitimate rights and interests."

4.2.2. Personal data rights protection is a prerequisite for establishing "digital trust" and ensuring the sustainable development of Digital Governments

Personal data protection is neither an impediment nor an incurred development cost, but a solid psychological and legal infrastructure cushion. Only when citizens are assured that their personal information will not be abused, monitored, or leaked will they proactively transition to interacting in the digital environment and become co-creators of data alongside local governments.

4.2.3. Exploiting data for socio-economic development must ensure a reasonable balance with the obligation to protect citizens' privacy rights

Personal data rights are not absolute rights and may be restricted by law for reasons of public interest and national security. Exploiting data flows to serve governance and digital

economic development must always proceed in tandem with proportionate rights-protection measures.

4.2.4. Personal data rights protection must decisively shift toward a "risk-based approach" centered on "proactive prevention"

Personal data protection must stay one step ahead by proactively identifying, assessing, and neutralizing potential risks to human rights right from the system design stage and throughout the entire data processing lifecycle.

4.2.5. State agencies' data governance authority must be tied to accountability and the obligations of transparency and openness

Acting in dual capacities as both a large-scale Data Controller and Data Processor, provincial governments must transition their legal compliance obligations from "passive commitments" to "proactive proofs" backed by specific technical and legal evidence. Any data processing behavior exceeding authorized purposes or causing data leakage must have official responsibilities clarified and be subjected to public oversight.

4.2.6. Personal data rights protection must ensure nationwide institutional uniformity while remaining flexible and tailored to local development particularities

Personal data protection standards mandated by the central level are uniform and supreme; provincial-level internal regulations are prohibited from contradicting or lowering these standards. Nevertheless, the enforcement process must feature a reasonable, flexible phased roadmap corresponding to the infrastructure level, budgetary capacity, and digital readiness of each locality.

4.2.7. The provincial data rights protection system must proactively approach and internalize advanced international standards

Amid international integration and high-quality FDI attraction, provincial governments must proactively reference and integrate advanced global data governance principles (such as the GDPR) into local practices.

4.3. Solutions for Protecting Personal Data Rights in Provincial-Level Digital Government Construction in Vietnam

4.3.1. Solutions for perfecting legal institutions and provincial internal regulations on personal data rights protection

(1) Advise and petition the central level to promulgate guiding circulars to resolve overlaps and inconsistencies between the Personal Data Protection Law and specialized laws. (2) Promulgate internal administrative Standard Operating Procedures (SOPs) on personal data protection applicable mandatorily to local cadres, civil servants, and public employees. (3) Promulgate internal management and operation regulations for Smart Operation Center (IOC) monitoring systems and pilot scheme reporting mechanisms submitted to competent authorities.

4.3.2. Solutions for enhancing organizational capacity and law enforcement personnel management in provincial-level digital government personal data protection

(1) Build an organizational model for a specialized Data Protection Unit and provincial DPO mechanism; ensuring professional independence within the framework of the single-leader system. (2) Assess human resources, operating costs, and the feasibility of phased implementation across localities.

4.3.3. Solutions for institutionalizing technical capability obligations and legal liabilities in provincial digital government personal data protection

(1) Mandate risk assessments, periodic security audits, and the individualization of system approval responsibilities. (2) Institutionalize the obligation of incident transparency and citizens' right to instant notification. (3) Standardize accountability obligations and immutable audit logging mechanisms to serve damage compensation. (4) Codify Citizen Rights Interactive Interfaces-transforming theoretical rights into technical tools.

4.3.4. Solutions for inspection, auditing, complaint and denunciation resolution, and delineating legal liability systems in personal data rights protection

(1) Establish independent, periodic, and ad-hoc cross-sectoral inspection mechanisms. (2) Clearly demarcate types of legal liabilities and grounds for holding heads of agencies accountable.

4.3.5. Solutions for guaranteeing data subjects' substantive rights based on the classification of Legal Bases for Data Processing

(1) Classify 3 groups of legal bases for data processing and corresponding structures of citizens' entitlements: Group 1: Data processing serving the execution of statutory tasks and authorities. Group 2: Data processing serving archival obligations and official dossiers. Group 3: Data processing based on citizens' voluntary consent.

(2) Standardized administrative-technical workflow for handling citizens' rights execution requests and resolving legal conflicts: Step 1- Subject reception and identification; Step 2 - Condition appraisal via the Legal Basis Filter; Step 3 - Technical execution and result feedback.

4.3.6. Solutions for innovating education and communication to raise awareness and legal self-defense capacity for data subjects

(1) Restructure communication content frameworks: Shift from technical operational guides to educating on rights and legal self-defense skills.

(2) Differentiate communication modalities by target demographic groups: (i) Vulnerable groups and rural/mountainous populations; (ii) Cadres, civil servants, and public employees directly processing dossiers; (iii) Students and youth.

(3) Establish communication efficacy evaluation mechanisms (KPIs) based on empirical surveys and social feedback: (i) Citizens' legal awareness index; (ii) Proactiveness in exercising self-defense rights; (iii) Minimized violation incident rates.

4.3.7. Solutions for data flow governance, public-private partnerships, and international experience

(1) Standardize public-private contract frameworks: Strictly demarcate legal status and bind contractor obligations: (i) Precisely define the legal status of subjects; (ii) Translate technical control rules into contractual obligation categories.

(2) Govern cloud computing infrastructure (Cloud) based on data classification levels and security risk assessments: (i) For core data and sensitive public authority data (civil status, identity, land, finance); (ii) For shared public service data and non-sensitive data; (iii) Strictly control cross-border data transfer mechanisms.

(3) Selectively absorb international experiences on data flow governance.

5. Implementation Roadmap for Data Rights Protection Solutions (Up to 2030)

Phase 1: Internal institutional standardization, technical process refinement, and apparatus optimization (2026-2027); *Phase 2:* Digitalizing proactive control processes and public-private partnership governance (2028-2029); *Phase 3:* Upgrading security infrastructure, narrowing the digital divide, and petitioning for national institutional perfection (Up to 2030).

CHAPTER 4 SUMMARY

The solutions proposed in Chapter 4 do not operate in isolation but are closely and dialectically bound together, forming an integrity of data governance that is honest, synchronized, and humane. This solution system resolves urgent practical bottlenecks of localities while contributing a comprehensive theoretical model to human rights legal science in Vietnam's digital era.

CONCLUSION

The research work "Protection of Personal Data Rights in the Construction of Provincial-Level Digital Government in Vietnam Today" represents a serious scientific endeavor aimed at resolving the dialectical relationship between administrative governance technology development and the guarantee of human rights and citizen rights in the digital space. Through theoretical research, practical investigation, and the formulation of a solution system, the thesis draws the following general conclusions: First, regarding legal science theory; Second, regarding the evaluation of local enforcement realities; Third, regarding the proposed solution system; Fourth, regarding the thesis's novel contributions and scientific significance. Personal data rights protection is not the endpoint of development, but the key unlocking the door to sustainable development-where technology is born to protect and promote the noble values of humanity.

LIST OF AUTHOR'S PUBLISHED SCIENTIFIC WORKS RELATED TO THE THESIS

[1] Cao Nguyen Hùng: "Current Legal Status of Personal Data Protection in Provincial-Level Digital Government Construction in Vietnam", Journal of Human Rights Law, No. 51 (December 2025).

[2] Cao Nguyen Hùng: "Personal Data Protection in Digital Government Construction – Lessons from the European Union and Implications for Vietnam", Electronic Communist Journal, January 23, 2026.

[3] Cao Nguyen Hùng: "Personal Data Protection in the European Union and Lessons for Vietnam", Electronic Communist Journal, March 1, 2026.