Challenges in building digital ethics for cadres and civil servants in state administrative agencies in the current context

Dr. Chu Thi Khanh Ly
Academy of Public Administration and Governance

Abstract: *Vietnam is entering a decisive phase of its National Digital Transformation, aimed at enhancing operational efficiency, improving public service quality, and ensuring transparency in the state administrative system. Alongside these opportunities, however, arise significant challenges concerning the digital ethics of cadres and civil servants. Key issues include the risks of misuse or leakage of sensitive personal data, inappropriate use of public information, administrative decision-making based on algorithms with potential bias, and unprofessional behavior on digital platforms. In this context, ethical, responsible, and integrity-based conduct in the digital environment is no longer theoretical but a critical requirement for maintaining public trust, ensuring business confidence, and safeguarding national security. This article examines the challenges that hinder the establishment and enforcement of digital ethics for cadres and civil servants, and proposes feasible solutions to promote a modern, efficient, transparent, and accountable digital public administration.*

Keywords: *Cadres, civil servants; digital ethics; state administration.*

1. Introduction

In the context of globalization and the Industrial Revolution 4.0, digital transformation has become an inevitable trend, exerting profound impacts on every aspect of socio-economic life, including operations of state administrative agencies. Vietnam is actively implementing its National Digital Transformation Program, aiming to establish a digital government, a digital economy, and a digital society. This process opens up numerous opportunities to enhance operational efficiency, improve the quality of public services, and strengthen the transparency and accountability of the administrative apparatus.

However, alongside these substantial benefits, digital transformation also poses unprecedented challenges, particularly in the field of ethics. The digital environment, with its decentralized nature, rapid dissemination of information, and the complexity of data and algorithms, has created numerous "gray areas" of

Received:
July 29, 2025
Revised:
August 29, 2025
Accepted:
September 23, 2025
https://doi.org
10.59394/JSM.85

ethics where traditional norms of conduct are insufficient to regulate behavior. For civil servants - the workforce directly responsible for operating the administrative system and delivering public services - the question of how to act ethically, responsibly, and with integrity in the digital environment is no longer a matter of choice, but an urgent requirement.

2. Digital ethics and the necessity of building digital ethics for cadres and civil servants in state administrative agencies

Digital ethics is defined as a system of ethical principles guiding the behavior of individuals and organizations in the digital environment. It encompasses the ways we design, use, share, and control digital technologies such as artificial intelligence (AI), big data, social networks, connected devices, and digital platforms (FMIT Institute, 2025).

In public administration, digital ethics is not a replacement but rather an essential extension and necessary complement to traditional norms of civil service ethics in the digital era. As stated, "civil service ethics are essentially the ethical standards of cadres and civil servants in the performance of their duties, which they must strictly comply with. If civil service is regarded as a profession, then civil service ethics constitute a form of professional ethics" (Ministry of Home Affairs, 2018). Civil service ethics thus form a system of values and standards that guide the conduct of cadres and civil servants in the performance of official duties. Accordingly, digital ethics in public administration can be understood as a set of ethical principles and norms that govern the actions of cadres and civil servants in carrying out their tasks and responsibilities in a digital environment.

Digital ethics in public administration includes standards such as compliance with the law, transparency, fairness, accountability, dedication, and respect for privacy and information security in online activities. These standards serve as guiding principles for all activities of cadres and civil servants in the digital environment, ensuring that civil service is conducted effectively, lawfully, and in accordance with ethical norms. The core principles of digital ethics in public administration include accountability, transparency, privacy and data protection, fairness, integrity, and social responsibility (Gorbatai, 2024).

Vietnam is entering a decisive stage of its National Digital Transformation process, aimed at improving operational efficiency, the quality of public services, and the transparency of the state administrative system. This process requires ethical, responsible, and integrity-based conduct in the digital environment. Any ethical violations, whether intentional or unintentional, not only cause material damage but also severely undermine the credibility of state agencies. Therefore, building digital ethics for cadres and civil servants in state administrative agencies is no longer a matter of theory but has become a vital requirement for maintaining public trust, safeguarding business confidence, and ensuring national security. The development of digital ethics for cadres and civil servants in state administrative agencies thus plays a vital role, specifically in the following aspects:

First, enhancing public trust in state administration. The digital environment facilitates more direct and transparent interactions between citizens and state agencies. However, public trust in state administration will be undermined if cadres and civil servants fail to comply with ethical standards while performing their duties online - such as leaking personal information, using official accounts for personal purposes, or showing disrespectful attitudes in digital interactions. Building digital ethics ensures transparency, fairness, and accountability of cadres and civil servants, thereby reinforcing citizens' and organizations' confidence in a service-oriented administration.

Second, ensuring information security and data protection. State administrative agencies

store and process a vast amount of critical data, including citizens' personal information and national secrets. Unethical digital practices, such as disclosing sensitive information, abusing data, or neglecting security protocols, can lead to severe consequences for both national security and individual privacy. Digital ethics requires cadres and civil servants to maintain a high sense of responsibility for information security, strictly comply with cybersecurity regulations, and contribute to safeguarding the digital assets of both the State and citizens.

Third, preventing corruption and misconduct in the digital environment. Without clear ethical rules, the digital space may open new loopholes for corrupt practices. Examples include abusing authority on electronic systems for personal gain, manipulating information, or accepting bribes through digital transactions. Establishing digital ethics helps define clear standards of integrity and non-self-interest in all digital activities of cadres and civil servants, thereby minimizing ethical and legal violations.

Fourth, improving operational efficiency and service quality. When cadres and civil servants adhere to digital ethical standards - such as using digital tools and platforms effectively and responsibly, complying with online working regulations, utilizing digital resources appropriately, and interacting professionally with colleagues and citizens - this practice fosters a modern, efficient, and high-quality digital working environment.

Fifth, preserving the image and reputation of state agencies. In the digital era, information spreads at lightning speed. Unethical behavior by cadres and civil servants in cyberspa`ce can quickly harm the image and reputation of individual agencies and, in some cases, the entire state administration. Building digital ethics shapes the proper conduct of cadres and civil servants in the digital environment, ensuring that all online activities reflect professionalism, integrity, and accountability, thus preserving and enhancing the reputation of state administrative agencies.

3. Challenges in building digital ethics for civil servants in state administrative agencies today

3.1. Challenges of awareness

One major challenge in the digital transformation of state administrative agencies is the issue of awareness regarding digital ethics and digital culture, both of which remain relatively new concepts. The shift in working methods has left many cadres and civil servants feeling "overwhelmed." Although digital technologies such as AI, chatbots, Big Data, "robot civil servants," and "virtual assistants" have been widely applied and brought about significant efficiency, they have simultaneously generated a range of new issues concerning civil service culture, digital culture, digital ethics, data governance, and digital human resources.

The core limitation lies in the perception of a portion of cadres and civil servants regarding the nature, role, and importance of digital transformation. Incomplete understanding has led to practices that are superficial, movement-based, inconsistent, partial, and not thoroughly implemented (Anh, 2025). This, in turn, limits their adaptability to the digital working environment and results in an inadequate understanding of digital ethical standards. Consequently, a sense of reluctance and a lack of readiness to adapt to rapid changes in the digital environment become prevalent. The lack of flexibility in learning and accepting new technologies poses a significant barrier to the adoption of digital ethics.

At a deeper level, traditional administrative mindsets remain prevalent, characterized by approaches such as "mandatory command," "ask–give mechanisms," "rigid principles," and "punishment or prohibition." Such mindsets hinder the transition toward more modern, flexible, collaborative, and dialogical approaches such as "dialogue, negotiation, cooperation, and connectivity." Although changing these mindsets is critically important for seizing opportunities and addressing challenges in the digital era, the transformation

process in the public sector remains relatively difficult and slow.

3.2. Institutional and legal challenges of digital ethics

The process of digital transformation in the public sector in Vietnam is facing significant challenges due to the absence and inadequacies of institutional and legal frameworks on digital ethics. The emergence of new, unprecedented social relations in the digital era has created numerous legal gaps, complicating state management and the development of digital ethical standards (Ministry of Science and Technology, 2023). Translating abstract ethical principles into binding codes of conduct in the digital environment remains a considerable challenge (Editverse, 2024).

First, Vietnam lacks a comprehensive and specialized legal framework on digital ethics that fully covers public sector activities. Existing regulations remain general, fragmented, and focused primarily on technical and security aspects although there are already several important legal documents - such as the 2018 Cybersecurity Law; the 2015 Law on Cyberinformation Security; Government Decree No. 53/2022/ND-CP dated September 15, 2022, detailing specific provisions of the Cybersecurity Law; the 2025 Personal Data Protection Law; and, Government Decree No. 137/2024/ND-CP dated October 23, 2024, on electronic transactions. The existing regulations fail to address in depth the complex ethical issues arising from digital transformation, particularly in the context of rapid AI development. As a result, state administrative agencies lack clear and consistent ethical guidelines for applying new technologies, leading to inconsistent interpretations and applications of principles, which in turn create risks in public governance and erode public trust in digital public services.

Second, a "legal vacuum" exists regarding AI ethics, algorithmic transparency, and accountability. Although the use of AI in the public sector (e.g., service provision, fraud detection) is becoming increasingly common, and the National AI Strategy to 2030 emphasizes ethics as a core pillar, specific legal instruments have not kept pace with this development. The 2018 Cybersecurity Law and Decree No. 53/2022/ND-CP dated August 15, 2022, does not provide detailed provisions on "AI fairness," "algorithmic transparency," or explicit "accountability" for AI systems. Similarly, the 2025 Personal Data Protection Law does not include specific rules for data protection in the context of new technologies such as big data, AI, or blockchain, nor does it adequately cover new categories of sensitive data (e.g., location, biometrics). This gap entails serious risks: the lack of algorithmic transparency may result in AI-driven decisions that are unfair or discriminatory, without mechanisms for explanation or traceability, directly affecting citizens' rights and eroding trust in digital government. Furthermore, the absence of clear accountability regulations leaves uncertainty over responsibility when AI causes harmful outcomes, undermining the ability to remedy mistakes and learn from failures (Diep, 2025). These shortcomings not only pose legal barriers but also threaten social justice, human rights, and public confidence in public administration in the digital era.

Third, there is a lack of detailed and mandatory legal provisions on Ethical Impact Assessment (EIA) and algorithm auditing. Although UNESCO has supported Vietnam in developing an AI ethics framework (Ministry of Science and Technology Media Center, 2025), no binding regulations currently require EIA for digital systems, particularly AI, prior to deployment in the public sector. This allows agencies to implement technologies without a comprehensive assessment of potential ethical risks and consequences. Furthermore, while legal instruments governing digital transformation - such as Decree No. 137/2024/ND-CP dated October 23, 2024, on electronic transactions in state agencies and information systems - address internal governance and electronic supervision,

they lack specific ethical requirements. As a result, digitalized operational processes are being established without clear ethical safeguards embedded from the outset. Although the 2025 Personal Data Protection Law is a significant step forward, it will only take effect in 2026, and detailed guiding decrees addressing complex aspects related to AI, big data, or sensitive data are still either pending or unclear. This creates both temporal and substantive gaps between the pace of actual digital transformation and the development of the necessary ethical and legal framework.

Fourth, in recent years, regulations on civil service ethics have been actively reviewed and supplemented, with notable documents such as the Prime Minister's Decision No. 1847/QD-TTg dated December 27, 2018, and the 2025 Law on Cadres and Civil Servants. However, these regulations still address public service performance in general terms only and do not contain specific provisions tailored to civil service ethics in the digital environment.

3.3. Challenges of capacity and skills

First, cadres and civil servants are facing overload and significant work pressure as they implement digital transformation. By nature, digital transformation requires that all procedures, workflows, and reports be conducted within digital environments, platforms, and infrastructures, which demand a wide range of complex skills. In particular, the digitization of documents consumes a considerable amount of time from civil servants. At the same time, the expansion of digital interaction channels between government and citizens (through innovative applications, portals, and electronic information pages) to improve speed and efficiency is becoming increasingly common. However, a considerable portion of cadres and civil servants struggle with this new way of working. Those accustomed to face-to-face interactions and paper-based processes often feel confused, pressured, and stressed when required to use digital technologies for interaction with citizens. This lack of adaptation not only creates difficulties for cadres and civil servants themselves but may also undermine efforts to improve the quality of citizen–government interactions (Anh, 2025).

Second, a shortage of highly qualified cadres and civil servants remains, as they are unable to meet the demands of working in the digital environment and keep pace with the rapid development of digital technologies. The rapid growth of digital technologies - such as the proliferation of artificial intelligence (AI) applications - has led some civil servants to rely heavily on technology without sufficient personal effort and commitment. AI has also contributed to the dehumanization of personal relationships, as specific human resource management processes can be performed entirely by machines, such as through the use of chatbots (Fritts & Cabrera, 2021). The use of AI by civil servants has consequently become increasingly common. However, concerns about the safety and ethics of AI use are growing, particularly given incidents of AI errors that have caused serious consequences.

Additionally, privacy and data protection remain significant challenges when deploying AI applications in the public sector (Mai & Vi, 2024). The combined impact of digital technologies and limitations in digital competence has led to low effectiveness in civil service performance. For example, although the SIPAS index has shown an upward trend in recent years, online public administrative services still face limitations that do not correspond with improvements in the SIPAS index. Specifically, the numbers of delayed procedures were 2,109 (31.51%) and 2,388 (35.1%) in 2023 and 2024 respectively (National Public Service Portal, 2025).

Furthermore, there remain significant challenges of human resources and technological capabilities. The limited number of AI specialists in the public sector results in a heavy reliance on the private sector. To utilize AI effectively, state agencies must enhance the

capabilities of their civil servants, leverage private-sector expertise, and foster collaboration among stakeholders in AI development (Diep, 2025). A significant challenge lies in the public sector's inability to attract and retain highly skilled technology professionals due to non-competitive salaries compared to those in the private sector. This has resulted in a shortage of experts in critical fields such as AI, cybersecurity, cloud computing, and data analytics (Huong, 2025).

Retraining programs are also costly, and a portion of cadres and civil servants remain reluctant or unprepared to adapt to the digital era (Huong, 2025).

3.4. Challenges of power abuse and "digital corruption"

The abuse of power and "digital corruption" is becoming increasingly complex in cyberspace. In sensitive sectors such as land, construction, and finance, unethical conduct in public service is becoming increasingly sophisticated and complex to detect in the digital environment, with "digital corruption" serving as a typical example. Manifestations of digital corruption include data manipulation, unauthorized prioritization of electronic dossiers, or creation of unnecessary technical barriers. Although digital technologies hold great potential for promoting transparency, they do not automatically prevent unethical behavior. Without robust management and monitoring mechanisms, digital tools may inadvertently create loopholes for corruption or privacy violations, undermining public trust.

Another serious risk is the use of deepfake technology, which produces highly sophisticated fake images, audio, and video that are nearly indistinguishable from authentic content. Deepfakes can be exploited to spread political misinformation, influence elections, sow social division, tarnish the reputation of leaders, or inflame geopolitical tensions, thereby threatening security and stability (Ministry of Science and Technology, 2024).

Vietnam has implemented the National Digital Transformation Program, as outlined in Decision No. 749/QD-TTg of the Prime Minister, which approves the "National Digital Transformation Program to 2025, with an orientation toward 2030." Despite progress in compliance with public service ethical standards among civil servants, corruption remains a serious challenge. For instance, Vietnam's Corruption Perceptions Index (CPI) score in 2023 was 41/100, ranking 83rd out of 180 countries, reflecting a decline compared with 2022. In 2024, the CPI further fell to 40/100, ranking 88th out of 180 countries, placing Vietnam among those still struggling with high levels of corruption (Transparency International, 2024).

3.5. Challenges of technological infrastructure and cybersecurity

Technological infrastructure of various state agencies remains outdated and fragmented. Many institutions continue to rely on legacy systems, making it challenging to integrate new digital solutions and hindering seamless information sharing (Huong, 2025). Moreover, "the provision of online public services by state agencies is still not convenient, user-friendly, or end-to-end; the rate of fully online procedures remains low; and, many applications and systems have been developed but remain fragmented, incomplete, and lacking in large-scale, shared digital platforms. Although having been generated, the data remains siloed, being neither interconnected nor fully exploited. The rollout of national databases has also been slow" (Ministry of Information and Communications, 2024).

According to the Ministry of Public Security, more than 48,500 Vietnamese ".vn" websites and portals were attacked, with over 4,000 of these targeting state agencies, between 2015 and 2021, and more than 350 cases of state secrets being leaked online occurred during the same period. The primary cause (57.7%) was the public posting of classified information on government websites or portals, particularly at local levels (provinces and districts). Leaks

through social media platforms (Facebook, Zalo, etc.) accounted for 9.3%, while the use of personal emails (Gmail, Yahoo Mail) to send or receive classified documents was also rising (1.6%) (Mai, 2023). In 2024, Vietnam experienced 3,900 cyberattacks, representing a 9.5% increase from 2022. Notably, 554 government (.gov.vn) and education (.edu.vn) websites were compromised with gambling malware. Over 83,000 computers and servers were infected with ransomware, an 8.4% increase. The leakage of personal data has reached alarming levels, contributing to a surge in online fraud cases (Ncsgroup, 2025). These figures underscore the increasing complexity of cybersecurity threats, necessitating stricter management and heightened awareness of information security across government agencies and organizations.

4. Solutions for building digital ethics for cadres and civil servants in state administrative agencies

Based on a comprehensive assessment of the challenges in establishing digital ethics in the public sector, the author proposes several solutions to strengthen digital ethics among civil servants, aiming toward a modern, efficient, integrity-based, accountable, and trustworthy digital public administration.

First, raising awareness and transforming mindsets. State administrative agencies should organize communication campaigns and specialized workshops to improve awareness of the importance of digital ethics, not only in terms of legal compliance but also as an ethical responsibility and a matter of public interest. This will help civil servants shift their management mindset from "administrative command" to "dialogue, cooperation, and connectivity," thereby maximizing the ethical potential of digital technologies.

Educational programs and communication efforts should focus on explaining how AI algorithms work, the risks of excessive exposure to personalized information, and how to identify and distinguish between false or misleading information related to Party guidelines and State policies. Furthermore, citizens should be encouraged to access diverse and reliable information sources and to develop critical thinking skills to evaluate information accurately. By doing so, they will be better equipped to protect themselves. Education and awareness campaigns should be integrated into curricula from an early age to help younger generations understand the importance of using AI responsibly and safely (Thanh, 2024). Reforming civil service ethics education should not only apply digital tools to teaching methods but also update contents to equip civil servants with knowledge and skills in "digital ethics," including responsible data use, information security, and ensuring fairness in digital systems. At the same time, state administrative agencies should foster a culture of innovation, encouraging cadres and civil servants to actively learn, adapt, and embrace new technologies instead of avoiding or resisting them.

Second, improving the legal and policy framework for digital ethics. Relevant authorities must review and supplement existing laws to ensure comprehensive, clear, and consistent regulations on issues such as personal data protection, cybersecurity, and emerging ethical challenges in civil service activities. This includes developing detailed codes of digital ethics tailored to different groups of cadres and civil servants and types of digital public services, based on principles of fairness, transparency, accountability, and privacy. Consideration should also be given to establishing a dedicated Digital Ethics Law or incorporating detailed provisions into existing laws, creating specialized units on AI ethics, integrating digital ethics into national curricula, and developing a responsible innovation ecosystem. The legal framework must include flexible updating mechanisms to respond to technological developments and new ethical challenges quickly. Vietnam can also learn from Singapore, which has developed the "AI Governance Framework" and "Model AI

Governance Guidelines," focusing on four core principles: fairness, transparency, human-centric approaches, and accountability (Personal Data Protection Commission Singapore, 2025). Vietnam should adopt a similarly proactive approach to creating practical guidelines and pilot mechanisms for AI applications in the public sector.

Third, developing comprehensive digital capacity and skills. Training and capacity-building institutions should design specialized programs on digital skills and digital ethics, emphasizing practical applications, responsible technology use, and addressing ethical dilemmas in the digital environment. State administrative agencies should ensure access to digital technologies and training for cadres and civil servants at all levels, particularly in rural areas and grassroots offices. In parallel, the capacity of cadres and civil servants to utilize data for policy-making, establish strategic digital governance mechanisms, and enhance digital skills should be developed not only for technical staff but also for policymakers and supervisors. Moreover, the public sector should fully leverage policies to attract and retain high-tech talents by improving compensation packages and creating an attractive working environment for specialists in AI, cybersecurity, and data analytics.

Fourth, strengthening monitoring mechanisms and accountability. The government should consider establishing independent data ethics councils or committees, with participation from experts, public representatives, and stakeholders, to provide advice, evaluation, and oversight of digital technology projects and digital ethics compliance. Mandatory tools, such as Ethical Impact Assessments (EIAs) and Data Protection Impact Assessments (DPIAs), should be applied to all major digital projects, particularly those involving sensitive data or algorithmic use. In addition, leadership and management should set an example by strictly adhering to and promoting digital ethics. Leaders must take the lead in using technology responsibly and transparently while firmly addressing digital ethical violations.

5. Conclusion

In the context of Vietnam's national digital transformation entering a decisive phase, establishing digital ethics for cadres and civil servants in state administrative agencies has become both an essential and urgent requirement. The challenges identified, ranging from issues of awareness, institutional and legal frameworks, capacity and skills, to the risks of power abuse, "digital corruption," and limitations in technological infrastructure, demonstrate that digital ethics is not merely a theoretical concern but also a pressing practical necessity. Without a strategic orientation and coordinated solutions, these shortcomings could directly undermine the effectiveness of public service delivery, erode public trust, and threaten social stability and safety.

To address these challenges, it is crucial to adopt a comprehensive set of solutions, including raising awareness and transforming civil servants' mindsets, improving the legal and policy framework on digital ethics, developing holistic digital capacity and skills, and strengthening mechanisms of monitoring and accountability. These measures will form the foundation for contributing to the development of a modern, transparent, effective, and integrity-based digital public administration. Ultimately, they will help reinforce public trust and provide a driving force for Vietnam's sustainable national development in the digital era.

References:

1. Anh, P. H. N. (2025). *Digital transformation in public service implementation of cadres and civil servants: An important driver for Ho Chi Minh City's development in the new context.* Retrieved from https://lyluanchinhtri.vn/chuyen-doi-so-trong-thuc-thi-cong-vu-cua-doi-ngu-can-bo-cong-chuc-dong-luc-quan-trong-thuc-day-phat-trien-thanh-pho-ho-chi-minh-trong-boi-canh-moi-6865.html

2. Diep, N. (2025). *AI application in Vietnam's public sector: Gaps, bottlenecks, and*

recommendations. Retrieved from https://ictvietnam.vn/ung-dung-ai-vao-khu-vuc-cong-tai-viet-nam-khoang-trong-diem-nghen-va-khuyen-nghi-69190.html

3. Editverse. (2024). *Ethical issues in considerable data research: Navigating challenges in 2024.* Retrieved from https://editverse.com/vi/ethical-issues-in-big-data-research-navigating-challenges-in-2024/

4. FMIT Institute. (2025). *What is digital ethics?* Retrieved from https://fmit.vn/en/glossary/dao-duc-so-la-gi

5. Fritts, M., & Cabrera, F. (2021). *AI recruitment algorithms and the dehumanization problem.* Ethics and Information Technology, 23(4), 791–801. https://doi.org/10.1007/s10676-021-09615-w

6. Gorbatai, A. (2022). *What is digital ethics?* Retrieved from https://www.vlerick.com/en/insights/what-is-digital-ethics/

7. Huong, N. (2025). *Challenges in Applying Technology in the Public Sector.* Retrieved from https://baophapluat.vn/nhung-thach-thuc-khi-ung-dung-cong-nghe-trong-linh-vuc-cong.html

8. Mai, C. (2023). *Raising awareness and responsibility in protecting state secrets.* Retrieved from https://nhandan.vn/nang-cao-y-thuc-trach-nhiem-trong-bao-ve-bi-mat-nha-nuoc-post755696.html

9. Mai, T. H., & Vi, L. H. (2024). *Artificial Intelligence and Public Sector Human Resource Development in Vietnam*. Retrieved from https://www.quanlynhanuoc.vn/2024/12/19/tri-tue-nhan-tao-va-phat-trien-nguon-nhan-luc-khu-vuc-cong-tai-viet-nam/

10. Ministry of Home Affairs. (2018). *Training materials on state management knowledge for cadres and civil servants.*

11. Ministry of Information and Communications. (2024). *Annual report 2024 and directions, tasks for 2025.*

12. Ministry of Science and Technology. (2024a). *Four ways to prevent and mitigate the impact of deepfakes in 2024.* Retrieved from https://mst.gov.vn/4-cach-de-ngan-chan-va-han-che-tac-dong-cua-deepfake-trong-nam-2024-19724 0723150839682.htm

13. Ministry of Science and Technology. (2024b). *Cybersecurity challenges and solutions in building a digital government today.* Retrieved from https://mst.gov.vn/thach-thuc-an-ninh-mang-va-giai-phap-trong-xay-dung-chinh-phu-so-hien-nay-197240815165720297.htm

14. Ministry of Science and Technology. (2023). *Improving training and capacity building for cadres and civil servants to meet digital transformation requirements.* Retrieved from http://cchccantho.gov.vn/nang-cao-hieu-qua-cong-tac-dao-tao-boi-duong-can-bo-cong-chuc-dap-ung-yeu-cau-chuyen-doi-so

15. Ministry of Science and Technology. (2025). *UNESCO supports Vietnam in building an ethical framework for artificial intelligence.* Retrieved from https://mst.gov.vn/unesco-ho-tro-viet-nam-ve-khung-dao-duc-cho-tri-tue-nhan-tao-19725052215 5855176.htm

16. National Assembly. (2015). *Law on Cyberinformation Security 2015.*

17. National Assembly. (2018). *Law on Cybersecurity 2018.*

18. National Assembly. (2025). *Law on Cadres and Civil Servants 2025.*

19. National Public Service Portal. (2025). *Index on serving citizens and businesses in administrative procedures and public services.* Retrieved from https://dichvucong.gov.vn/p/home/dvc-index-tinhthanhpho-dvctructuyen.html

20. Ncsgroup. (2025). *Vietnam Cybersecurity Review 2023 and Forecast 2024.* Retrieved from https://ncsgroup.vn/tong-ket-an-ninh-mang-viet-nam-nam-2023-va-du-bao-2024

21. Personal Data Protection Commission Singapore. (2025). *Singapore's approach to AI governance.* Retrieved from https://www.pdpc.gov.sg/model-ai-gov

22. Prime Minister. (2018). *Decision No. 1847/QD-TTg approving the public service culture scheme.*

23. Thanh, N. C. (2024). *Artificial intelligence and challenges to protecting the Party's ideological foundation today.* Retrieved from https://www.tapchicongsan.org.vn/web/guest/dau-tranh-phan-bac-cac-luan-dieu-sai-trai-thu-dich/chi-tiet/-/asset_publisher/YqSB2JpnYto9/content/tri-tue-nhan-tao-va-nhung-nguy-co-thach-thuc-doi-voi-cong-tac-bao-ve-nen-tang-tu-tuong-cua-dang-hien-nay

24. Transparency International. (2024). *Corruption Perceptions Index.* Retrieved from https://www.transparency.org/en/countries/vietnam