Modern public administration and legal adaptation in the digital age and a case study of Thailand

Thipaporn Klawklong

[1,2] Department of Law, Faculty of Humanities and Social Sciences, Sakon Nakhon Rajabhat
* Corresponding author's e-mail: thipaporn2564@gmail.com

ABSTRACT

Thailand is experiencing significant technological changes in the digital era that directly impact public administration, especially Thai legal frameworks. This academic article aims to 1) analyze the necessity for Thai laws to adapt to the digital transition and 2) explore legal issues and propose approaches to improve laws in alignment with digital-age public administration. The study findings indicate that 1) the government's digital transformation affects numerous laws, as Thai legislation tends to be outdated and unable to keep pace with change. This necessitates legal improvements across multiple domains, from personal data protection, cybersecurity, and electronic transactions to online crimes, digital economy, and workers' rights to appropriately support technological changes. 2) To ensure laws can effectively respond to global changes, the government should modernize Thai legislation to align with the digital world, particularly in seven key areas: (1) Personal Data Protection Law, (2) Cybersecurity Law, (3) Digital Economy and Platform Taxation Law, (4) Platform Labor Law, (5) Artificial Intelligence and Technology Ethics Law, (6) Cross-Border Data Governance Law, and (7) Online Crime Law. These legal improvement frameworks will help the government adapt to global conditions in a timely manner, enhance citizen protection, and enable the state to manage the economy and national security efficiently, creating stability for both government and citizens as Thailand transitions to modern public administration in a peaceful and secure manner.

Introduction

The world is fully entering the digital age. Information technology, artificial intelligence (AI), blockchain, and big data are becoming crucial factors transforming economic structures, society, and public administration. The reformation of Thailand into Digital Thailand envisions a country that can create and fully utilize digital technology to develop infrastructure, data, innovation, human resources, and other assets to drive economic development toward security, prosperity, and sustainability.

Governments worldwide, including Thailand, are adapting to use digital technology in providing public services, reducing bureaucratic procedures, and increasing national administration efficiency. However, this transformation brings complex legal challenges, as laws are the source of authority that enables smooth and effective administration.

When governments implement technology, existing laws may be insufficient to address new problems such as personal data protection, cybersecurity, electronic transactions, electronic crime, and labor rights in the platform economy. The key question is "In which direction should laws proceed?" As the world and Thailand are driven by digital transformation, how should the state improve laws to balance innovation and citizen rights protection?

This article analyzes technological changes in the digital era that directly impact public administration, particularly their effect on Thai law. It examines the necessity for legal adaptation to the digital transition as the government must adapt to efficiently use digital technology in public service delivery. Meanwhile, existing laws may not cover or align with the changing global context. The article explores approaches the state should implement to enable laws to effectively support the digital transition, including studying legal directional changes, examining legal issues, and proposing legal improvement frameworks to help Thailand keep pace with global changes and build sustainability in the digital age. The article has two objectives: 1) to analyze the necessity for Thai laws to adapt to the digital transition, and 2) to explore legal issues and propose approaches to improve laws in alignment with public administration in the digital age.

Digital transformation

Digital Government or E-Government refers to the use of digital technology, especially information and communications technology (ICT), to enhance efficiency, transparency, and accessibility of government services. It aims to improve citizens' quality of life, administration, and social development in ways that respond to the needs of citizens and businesses (United Nations, 2020). Many government policies designed for citizens are already transitioning to digital government, such as the Digital Wallet Policy, which promotes financial technology use and stimulates the economy through a "digital wallet" system for distributing funds or benefits to citizens, particularly in the form of subsidies or economic stimulus programs (Chuenudomsavad, 2023), while ensuring transparency in government budget expenditure.

Technological changes in the digital era directly impact public administration and domestic law. Governments must adapt to efficiently incorporate digital technology in administration and public services. Digital has become a key driver of government and society today. Digital technology has become a significant variable changing how governments operate, especially in public administration and service delivery (Mergel, Edelmann, & Haug, 2019). The transition to modern public administration or digital government leads to increased efficiency, transparency, reduced inequality, and greater citizen participation. However, this process comes with challenges such as digital inequality and cybersecurity issues (OECD, 2020), and governments continue to undergo multifaceted changes toward becoming digital governments.

Current technological changes in government

Technology is rapidly evolving and impacts multiple dimensions of daily life, economy, and society. Key examples of technological changes in government include:

Artificial intelligence (AI): AI has taken on significant roles across various industries such as medicine, finance, and manufacturing by increasing efficiency and accuracy through in-depth data analysis and chatbot services (Cheng et al., 2020).

Internet of things (IoT): IoT enables seamless device connectivity and machine-to-machine communication, such as public CCTV system control and smart homes that can control electricity and appliances via smartphones (Atzori, Iera, & Morabito, 2017).

Wireless communication: 5G technology increases communication speed and reduces latency, making it suitable for applications like video conferencing, internet education, and remote surgery (Lu et al., 2019).

Digital transformation: Organizations and businesses are accelerating digital adaptation by using cloud platforms alongside big data processing to create competitive advantages (Vial, 2019).

Blockchain: Blockchain technology is applied across multiple sectors including finance, supply chain management, and identity verification due to its data security and transparency (Zheng et al., 2018), such as the Digital Wallet project.

The government's digital transformation significantly impacts government adaptation and multiple sectors, particularly affecting laws and regulations across several domains that must rapidly adapt for appropriate enforcement, from data privacy and cybersecurity to new legal frameworks necessary for government operations in the digital age.

Factors driving legal directional changes

1. **Legal adaptation to support government digital services**: Governments worldwide have restructured public service delivery toward digital formats, necessitating improvements to electronic transaction laws, such as electronic signature laws and digital government service laws (Lindgren & Jansson, 2013).

2. **Impact on personal data laws**: Digital governments must manage vast amounts of citizen data, leading to concerns about personal data protection. Related laws such as the GDPR in Europe or PDPA in Thailand are enforced to regulate the collection and use of data by government agencies (European Parliament, 2016).

3. **Cybersecurity and related laws**: As governments increasingly use digital technology, cybersecurity risks also increase, necessitating the enactment of controlling laws and measures, such as Thailand's Cybersecurity Act or the United States' Cybersecurity Act (Kshetri, 2017).

4. **Laws regarding artificial intelligence (ai) and automated decision-making**: The implementation of AI in government decision-making processes, such as in justice systems and public administration, raises legal questions about transparency, accountability, and algorithmic bias (Wirtz et al., 2019).

5. **Impact on labor laws and government employment**: The use of digital technology and automated systems may change government employment structures, affecting labor law and the rights of government employees in the digital age (OECD, 2020).

6. **Increasingly complex legal interpretation**: The use of AI and algorithms in the justice process, such as automated case consideration and digital evidence analysis, creates challenges in legal interpretation and protection of citizens' rights. For example, AI used to analyze suspect risk in U.S. legal proceedings has been criticized for bias against certain ethnic groups (Goodman & Flaxman, 2017).

7. **Staying ahead of online fraud**: Online crime has evolved into various forms with numerous channels for deceiving citizens, resulting in enormous benefits from technology-based fraud.

In summary, the government's digital transition and modern public administration require continuous legal adaptation to accommodate technological changes, from laws concerning personal data, cybersecurity, and online crime to laws related to AI and labor. The digital transformation significantly impacts legal systems worldwide, necessitating the adaptation of Thai legal dimensions to respond to emerging challenges and opportunities and comprehensively protect citizens in a rapidly changing environment.

Origins of Thai law

Thai law derives from multiple sources, including ancient indigenous law, foreign legal influences, and contemporary legislative processes. The main sources of Thai law can be divided into five categories

1. **Customary law**: Before the written legal system, Thai law was based on Thai social.

2. **Customs**, which served as rules for governing and adjudicating cases, especially during the Sukhothai and Ayutthaya periods. For example, the "Three Seals Law" enacted during the reign of Rama I compiled legal principles rooted in original customs (Somchai, 2015).

3. **Statutory law**: Laws enacted by the state are the main source of Thai law today, including the Constitution, Acts, Emergency Decrees, Royal Decrees, Ministerial Regulations, and announcements from various state agencies. For example, the Civil and Commercial Code, which was influenced by European law, especially French and German civil law (Paiboon, 2018).

4. **Case law or judicial precedents**: In some cases, court judgments, especially Supreme Court and Constitutional Court rulings, can serve as guidelines for legal interpretation and enforcement. Although Thailand does not use a common law system, court judgments are often used as standards in considering similar cases (Vorachet, 2019).

5. **International law**: Thailand is a party to many international treaties and conventions, such as the Convention on the Rights of the Child (CRC) and the World Trade Organization (WTO) international trade law. These laws influence the improvement of Thai law to align with international standards (Pracha, 2020).

6. **General principles of law**: General legal principles such as justice, equality, and rule of law are important guidelines in developing Thai law in accordance with international rule of law principles (Apirat, 2021).

In summary, Thai law originates from a combination of customary law, state-enacted law, court judgments, international law, and general legal principles, all of which play important roles in determining the current legal framework of Thailand. These laws tend to remain in traditional forms, with some laws dating back to 1957, which are now outdated. Some are unsuitable for addressing current global problems or new crimes, as criminals themselves have developed sophisticated methods, including electronic crimes that use cyber technology as a key tool. All of these factors highlight the necessity for laws to adapt as current protection becomes insufficient.

The necessity for legal improvement in government digital transformation

The digital transformation of government is a process that introduces digital technology into public administration, impacting laws in multiple ways. The necessity for legal improvement to support this transformation can be summarized as follows

3.1 Personal Data Protection and Privacy: Digital governments must collect and use vast amounts of citizen data, creating risks to privacy and personal data rights violations. Therefore, laws must be improved to align with international standards, such as Thailand's Personal Data Protection Act B.E. 2562 (PDPA), which is based on Europe's General Data Protection Regulation (GDPR) (Westby, 2020).

3.2 Cybersecurity: Cyber threats such as attacks on state digital infrastructure, data hacking, and malware are increasing, necessitating improvements to cybersecurity laws like Thailand's Cybersecurity Act B.E. 2562 to establish preventive measures and responses to emerging threats (NIST, 2018).

3.3 Identity Verification and Electronic Transactions: Digital governments must facilitate secure online transactions for citizens, such as digital identity verification and electronic signatures to simplify and expedite public services. This requires updating the Electronic Transactions Act B.E. 2544 to align with international standards like the European Union's eIDAS (European Commission, 2021).

3.4 Government Law Improvement to Support Digital Administration: The use of artificial intelligence (AI) and Big Data in public administration requires new legislation for regulation, empowerment, and duties, such as e-Government laws that establish standards for government data and technology use, like Estonia's advanced e-Government system (Margetts & Dunleavy, 2013).

3.5 Digital Economy and Online Platform Control: The state must regulate digital transactions such as e-Commerce, Cryptocurrency, and Smart Contracts, necessitating improvements to the Digital Asset Business Act B.E. 2561 and the Anti-Money Laundering Act B.E. 2542 to accommodate advanced financial technologies (Brynjolfsson & McAfee, 2014).

3.6 Labor Law and Labor Rights in the Digital Age: Digital platforms like Grab and Uber have created a "Gig Economy" where workers have different working patterns than before. This requires

updating the Labor Relations Act B.E. 2518 and the Social Security Act B.E. 2533 to accommodate digital labor rights (De Stefano, 2016).

3.7 Legal Improvement to Promote Good Governance and Transparency: Digital governments must use open data systems and AI in providing public services but require controlling laws to prevent corruption. The Official Information Act B.E. 2540 should be improved to facilitate technology use in controlling and accessing government information (Meijer, 2015).

3.8 Keeping Pace with Technological Crime Control: To stay current with responses to and punishment of criminals who use computer and cyber channels to commit crimes in various forms that older laws cannot adequately address.

In summary, the government's digital transformation and modern public administration necessitate legal improvement in many areas. Thai law tends to be outdated and unable to keep pace with change, creating a need for adaptation. The impact of the digital transition significantly affects Thai law, influencing multiple laws from personal data protection, cybersecurity, electronic transactions, and online crime to the digital economy and labor rights. These improvements will allow laws to appropriately support technological changes and create security for both the government and citizens in Thailand's transition to modern public administration.

Concepts and theories regarding government digital transformation and law

The transition to digital government (E-Government) is a process where the public sector implements digital technology in various operations to increase operational efficiency and public service delivery, directly impacting existing legal frameworks and regulations. We must examine which concepts and theories relate to the government's digital transformation and its impact on law.

1. Concepts and theories related to this issue include:

1.1 Digital government theory: This theory discusses the implementation of information and communication technology in the public sector to increase efficiency, transparency, and public participation. However, introducing digital systems requires improving related laws, such as electronic transaction laws and personal data protection laws (Dunleavy et al., 2006).

1.2 Digital governance and regulation theory: This concept addresses the government's need to create new regulations to govern digital technology such as artificial intelligence (AI), blockchain, and cybersecurity. The state must consider legal issues including privacy rights, transparency, and legal accountability (Cordella & Paletti, 2019).

1.3 Sociotechnical systems theory: This theory explains that technological changes impact social systems and laws. Governments implementing digital technology must adjust policies and laws to suit the new context, such as labor laws for digital platforms and cybersecurity laws (Bostrom & Heinen, 1977).

1.4 Digital economy and law theory: This theory views digital transformation as making the economy and society increasingly dependent on technology, requiring new laws to support digital transaction formats, such as laws regarding smart contracts and consumer protection in digital markets (Brynjolfsson & McAfee, 2014).

1.5 Cybersecurity and law theory: The transition to digital government increases cybersecurity threats, requiring governments to establish laws and measures to address cybersecurity risks, such as Thailand's Cybersecurity Act and personal data protection laws (NIST, 2018).

In summary, considering digital governance and regulation theory, which addresses the government's need to create new regulations to govern digital technology, alongside digital government theory and sociotechnical systems theory, which discuss the need to improve relevant laws when implementing digital systems, results in the necessity to improve laws across multiple domains. These range from personal data control and cybersecurity through cybersecurity and law theory to the digital economy and labor in the digital age from digital economy and law theory. These concepts and theories help explain

the relationship between technology and law, which is a crucial factor that the state must consider in implementing legal policies.

2. Research studying the impact of government digital transformation on law

(Academic Bureau, Secretariat of the House of Representatives, 2016): This research studies the adaptation of Thai government organizations in the transition to digital government, focusing on improving laws and regulations to support digital technology use in the public sector.

(Dharin Lerdsukeekasem, 2022): This research focuses on studying the adaptation process of Thailand's Ministry of Foreign Affairs in implementing digital technology, considering the improvement of relevant laws and policies to support operations in the digital age.

Digital Transformation of Public Organizations to Enhance Competitiveness: This research surveys factors affecting the success and obstacles of digital transformation in Thai public organizations, focusing on improving laws and regulations to facilitate digital technology implementation.

(Koonchorchai, A, 2021): This research studies factors affecting the success and obstacles in the digital transformation of the Bangkok Metropolitan Administration's Foreign Affairs Office, finding that improving relevant laws and policies is a crucial factor influencing the success of such transformation.

In summary, related research shows that in the transition to digital government, the adaptation of public organizations to the digital government era, with emphasis on improving laws, regulations, and relevant policies, is a key factor contributing to success.

Legal issues and improvement approach to keep pace with digital age changes

Technological changes in the digital age affect existing laws in many ways that may not effectively accommodate new situations, causing many countries including Thailand to improve their laws to appropriately support these changes. From surveying legal issues, key areas requiring improvement to modernize Thai law and effectively protect citizens' rights include:

1. Legal issues requiring improvement to keep pace with digital age changes

1.1 Personal data protection laws and privacy

Issue: Digital technology use results in personal data being collected, analyzed, used, and disseminated for business purposes and state security. Without adequate protection measures, this may impact citizens' privacy and security from personal data theft by criminal groups. Personal data requires strict control to prevent citizens' rights violations.

Improvement Approach: The Personal Data Protection Act B.E. 2562 (PDPA) enforcement still faces understanding and compliance problems among public and private organizations (Westby, 2020). Clearer practical guidelines for public and private sectors should be established, measures for overseeing AI and Big Data use in personal data processing should be defined, stronger penalties for data violations should be reinforced, and mechanisms for civil litigation to protect citizens' rights and claim exemplary damages should be increased.

Reference Example: The European Union's General Data Protection Regulation (GDPR), an international standard for personal data protection law (European Parliament & Council of the European Union, 2016).

1.2 Cybersecurity laws

Issue: Cyber threats such as attacks on critical infrastructure, government data hacking, and malware release have led many countries to enact laws protecting their digital infrastructure. Thailand's law focuses on protecting critical information infrastructure. However, this law lacks clear guidelines for protecting the private sector and citizens from cyber threats (NIST, 2018). Cybersecurity law enactment must balance state security with citizens' privacy rights, as many countries use these laws as tools for citizen surveillance (Zuboff, 2019).

Improvement Approach: Review the Cybersecurity Act B.E. 2562 to balance state security and citizens' rights, improve real-time cyber threat notification and response mechanisms, update cybersecurity

laws to accommodate more complex threats, and establish cybersecurity standards for public and private organizations following the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Reference Example: The European Union Cybersecurity Act, which focuses on certifying the security of digital infrastructure (European Parliament & Council of the European Union, 2019).

1.3 Digital economy and platform taxation laws

Issue: Platform businesses like Shopee, Lazada, Facebook, and Google earn enormous revenues from users in the country but are not clearly subject to Thai tax laws, causing the state to lose significant revenue sourced from within Thailand.

Improvement Approach: Enforce Digital Services Tax (DST) for multinational platform companies, improve e-Commerce tax laws to ensure foreign platforms earning revenue from Thai people pay taxes in Thailand, and promote laws regarding digital assets and cryptocurrencies to control money laundering and prevent tax evasion.

The European Union and many countries have begun using Digital Services Tax (DST) to collect taxes from digital companies like Google, Amazon, and Facebook that provide services in the country but are not registered there (Brynjolfsson & McAfee, 2014).

Reference Example: OECD Model Rules for Digital Taxation, which provide guidelines for taxing multinational digital businesses (OECD, 2021).

1.4 Platform economy and labor laws

Issue: Workers in the platform economy, such as Grab drivers, food delivery riders, and online freelancers, do not receive benefits or protection under traditional labor laws. In some countries like the United Kingdom, courts have ruled that Uber drivers are "employees" entitled to labor rights, while in other countries, platform workers are classified as "independent contractors" (De Stefano, 2016).

Improvement Approach: Define and amend legal terminology in labor laws to ensure workers from all platforms receive minimum benefits such as social security and termination compensation, improve the Labor Protection Act B.E. 2541 to accommodate new employment forms in the digital age, and study approaches of European Union labor laws that define Uber drivers and platform workers as "employees" entitled to benefits.

Reference Example: UK Supreme Court Ruling on Uber (2021), which ruled that Uber drivers are employees entitled to benefits.

1.5 Artificial intelligence and digital ethics laws

Issue: AI and algorithms are used in public and private sector decision-making processes, such as loan approval, job application screening, and crime detection, which may impact fairness and individuals' human rights.

Improvement Approach: Enact laws to regulate AI use in the public sector to prevent algorithmic bias, require technology platforms to disclose AI operating principles to the public for transparency, and promote AI ethical frameworks following UNESCO and European Union guidelines.

Reference Example: European Union AI Act, the world's first law strictly regulating AI use (European Parliament & Council of the European Union, 2024).

1.6 Cross-border data governance laws

Issue: To prevent transnational crime, the flow of data between countries remains problematic as each country has different data control laws, creating limitations on cross-border data use (Greenleaf, 2019).

Improvement Approach: Improve laws regarding transnational crime or the Penal Code (No. 10, B.E. 2545) to be clear, comprehensive, and consistent with international standards for laws emphasizing strict personal data protection while allowing international data flow (Greenleaf, G., 2019).

Reference Example: Improving domestic laws to align with standards set by international organizations, GDPR (General Data Protection Regulation) of the European Union, or the APEC Cross-Border Privacy Rules (CBPR) framework.

1.7 Online crime laws

Issue: Online crime (Cybercrime) continuously evolves with advancing technology, such as online fraud, cyber-attacks, and personal data breaches, which existing laws may not effectively address with changing threats.

Improvement Approach: Laws regarding online crime, the Emergency Decree on Prevention and Suppression of Technology Crime B.E. 2566, or the Penal Code B.E. 2545, must be updated to keep pace with technological changes and cybercriminal behavior. These legal improvements will help more effectively prevent and enforce laws, such as implementing appropriate penalties for serious cybercrimes.

Reference Example: Effective enforcement, modern laws can help law enforcement agencies appropriately manage cyber criminals (Davis, 2022). Singapore has improved computer crime laws to increase penalties (Government of Singapore, 2021), and the United States has passed the Cybersecurity Maturity Model Certification (CMMC) to elevate cybersecurity standards (U.S. Department of Defense, 2020).

The above represents legal issues requiring improvement and suggested improvement approaches, along with references to noteworthy model laws.

2. Recommendations

As Thailand and its government transition to digital government, to ensure laws can accommodate digital age changes, it is recommended that the government consider improving laws to align with the digital world, particularly in seven areas:

(1) Personal Data Protection Laws: Improve the Personal Data Protection Act B.E. 2562. PDPA enforcement should promote understanding and compliance among public and private organizations.

(2) Cybersecurity Laws: Review the Cybersecurity Act B.E. 2562 to balance state security and citizens' rights, improve cyber threat notification and response mechanisms, and update cybersecurity laws to accommodate more complex threats.

(3) Digital Economy and Platform Taxation Laws: Enforce Digital Services Tax (DST) for multinational platform companies and improve e-Commerce tax laws to ensure foreign platforms earning revenue from Thai people pay taxes in Thailand.

(4) Platform Labor Laws: Define and amend legal terminology in labor laws to ensure workers from all platforms receive minimum benefits such as social security and termination compensation, and improve the Labor Protection Act B.E. 2541 to accommodate new employment forms in the digital age.

(5) Artificial Intelligence and Technology Ethics Laws: Enact laws to regulate AI use in the public sector to prevent algorithmic bias, require technology platforms to disclose AI operating principles to the public for transparency, and promote AI ethical frameworks following UNESCO and European Union guidelines.

(6) Cross-Border Data Governance Laws: Improve laws regarding transnational crime, such as the Penal Code B.E. 2545, to be clear, comprehensive, and consistent with international standards for laws emphasizing strict personal data protection.

(7) Online Crime Laws: Update laws to keep pace with technological changes and cyber-criminal behavior. Improving laws like the Emergency Decree on Prevention and Suppression of Technology Crime B.E. 2566 or the Penal Code B.E. 2545 will help more effectively prevent and enforce laws.

These seven issues are pilot legal improvement approach recommendations that should be prioritized, serving as important tools to help the government adapt to global situations in a timely manner and create fairness for citizens in the digital age. Updating laws to keep pace with technology not only helps protect citizens' rights but also helps the state efficiently manage the economy and national security.

Analysis

The transition to digital government requires continuous legal adaptation to accommodate technological changes. The digital transformation significantly impacts legal systems worldwide, including

Thailand's legal dimensions, which must adapt to respond to challenges and embrace emerging opportunities, enhancing citizen protection comprehensively to keep pace with changing situations.

Since Thai law has diverse origins, such as a combination of customary law, state-enacted law, court judgments, international law, and general legal principles, all of which play important roles in determining Thailand's current legal framework, which tends to remain in traditional forms with some laws being ancient and having outdated criteria or procedures. Some laws were enacted decades ago, such as the Civil and Commercial Code (effective since 1925) and the Penal Code (effective since 1956). Despite some amendments, many core principles remain unchanged and are now outdated. Some are unsuitable for addressing current global problems or new crimes, as criminals themselves have developed sophisticated methods, including electronic crimes that use cyber technology as a key tool. The above highlights the necessity for Thai law to adapt, continuously adapting to accommodate technological changes until it can appropriately protect citizens.

Thai law tends to be outdated and unable to keep pace with change, creating a government need to improve laws in many areas, as the impact of the digital transition significantly affects Thai law, influencing multiple laws. Considering digital governance and regulation theory, which addresses the government's need to create new regulations to govern digital technology, alongside digital government theory and sociotechnical systems theory, which discuss the need to improve relevant laws when implementing digital systems, results in the necessity to improve laws across multiple domains. These range from personal data control, cybersecurity through cybersecurity and law theory, to the digital economy and labor in the digital age from digital economy and law theory. Related research also suggests that in the transition to digital government, the adaptation of public organizations to the digital government era, with emphasis on improving laws, regulations, and relevant policies, is a key factor contributing to improved adaptation success.

Table 1 Summarizing analysis results and surveyed laws requiring improvement

No.	Law	Issue	Improvement approach	Reference example
1	Personal Data Protection Laws	Data theft security risk without adequate protection measures may impact citizens' privacy.	Establish AI and Big Data oversight measures in personal data processing, strengthen penalties for data violations.	European Union's General Data Protection Regulation (GDPR), an international standard for personal data protection.
2	Cybersecurity Laws	Law lacks clear guidelines for protecting the private sector and citizens from cyber threats.	Review the Cybersecurity Act B.E. 2562 to balance state security and citizens' rights.	European Union Cybersecurity Act, which focuses on certifying digital infrastructure security.
3	Digital Economy and Platform Taxation Laws	Platform businesses like Shopee, Lazada, Facebook, and Google earn enormous revenues but are not clearly subject to Thai tax laws	Collect taxes from multinational technology companies using Digital Services Tax (DST) for digital companies providing services without registering in the country.	OECD Model Rules for Digital Taxation, guidelines for taxing multinational digital businesses.
4	Platform Labor Laws	Platform economy workers like Grab drivers, food delivery riders, and online freelancers lack traditional labor law benefits.	Define and amend legal terminology to ensure all platform workers receive minimum benefits like social security and termination compensation, improve the	UK Supreme Court Ruling on Uber (2021), which ruled that Uber drivers are employees entitled to benefits.

			Labor Protection Act B.E. 2541.	
5	Artificial Intelligence and Technology Ethics Laws	Algorithms in public and private sector decision-making may impact fairness and individual human rights.	Enact laws regulating public sector AI use to prevent algorithmic bias, require technology platforms to disclose AI principles for transparency, promote AI ethical frameworks.	European Union AI Act, the world's first law strictly regulating AI use.
6	Cross-Border Data Governance Laws	Transnational crime prevention and international data flow face issues with differing country data control laws.	Improve transnational crime laws or Penal Code B.E. 2545 to be clear, comprehensive, and aligned with international standards emphasizing strict data protection.	Domestic law improvements aligning with standards from international organizations, GDPR of the European Union.
7	Online Crime Laws	Online crime continuously evolves with technology advances, including online fraud, cyber-attacks, and data breaches that existing laws may not effectively address.	Update Technology Crime Prevention and Suppression Emergency Decree B.E. 2566 or Penal Code B.E. 2545 to keep pace with technological changes and cyber-criminal behavior, implement appropriate penalties.	Singapore improved computer crime laws to increase penalties, and the US passed the Cybersecurity Maturity Model Certification (CMMC) to elevate cybersecurity standards.

Conclusion

From the above, it can be concluded that modern public administration and legal adaptation, regarding which direction laws should proceed in the digital age, requires the government to improve laws to align with the digital world. The study surveyed legal issues that should be prioritized for improvement, particularly in seven main areas: (1) Personal Data Protection Laws, (2) Cybersecurity Laws, (3) Digital Economy and Platform Taxation Laws, (4) Platform Labor Laws, (5) Artificial Intelligence and Technology Ethics Laws, (6) Cross-Border Data Governance Laws, and (7) Online Crime Laws. These preliminary legal improvement approach recommendations will help the government adapt to global situations in a timely manner and create fairness for citizens in the digital age. Updating laws to keep pace with technology and the complexity of crime not only helps protect citizens' rights but also helps the state efficiently manage the economy and ensure national security, creating stability for both the government and citizens as Thailand transitions to modern public administration in a peaceful and secure manner.
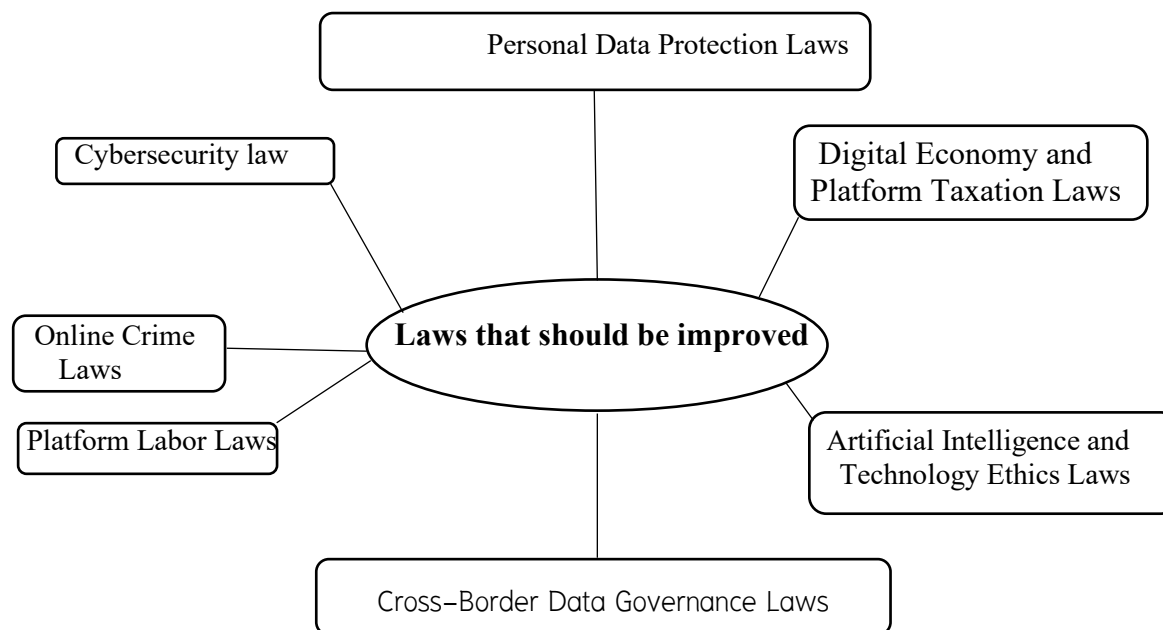
Diagram1: Summary of suggestions

References

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A sociotechnical perspective. *MIS Quarterly*, 1(3), 17-32. https://doi.org/10.2307/248710

Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. W.W. Norton & Company.

Cordella, A., & Paletti, A. (2019). Government as a platform, orchestration, and public value creation: The case of the United Kingdom's Government Digital Service. *Government Information Quarterly*, 36(4), 101421. https://doi.org/10.1016/j.giq.2019.101421

Davis, M. (2022). Cybersecurity law and enforcement: Challenges and solutions. *Cyber Law Journal*, 45(2), 120-135.

De Stefano, V. (2016). The rise of the "just-in-time workforce": On-demand work, crowd work, and labor protection in the gig economy. *Comparative Labor Law & Policy Journal*, 37(3),461-471.

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). Digital era governance: *IT corporations, the state, and e-government*. Oxford University Press.

European Commission. (2021). *Electronic identification and trust services (eIDAS)*. https://digital-strategy.ec.europa.eu/en/policies/eidas

European Parliament, & Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR). Official Journal of the European Union.*

European Parliament, & Council of the European Union. (2019). *Regulation (EU) 2019/881 on ENISA the European Union Agency for Cybersecurity) and on information and*

communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151, 15–69. https://eur-lex.europa.eu/eli/reg/2019/881/oj

Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a "right to explanation." *AI Magazine*, 38(3), 50-57.

Greenleaf, G. (2019). Global data privacy laws 2019: Forty years of evolution and future challenges. *University of New South Wales Law Journal*, 42(3), 1005–1042. https://doi.org/10.2139/ssrn.3434629

Kshetri, N. (2017). The evolution of cybersecurity regulations. *IT Professional*, 19(2), 6-9. https://doi.org/10.1109/MITP.2017.23

Lindgren, I., & Jansson, G. (2013). Electronic services in the public sector: A conceptual framework. *Government Information Quarterly*, 30(2), 163-172. https://doi.org/10.1016/j.giq.2012.10.005

Margetts, H., & Dunleavy, P. (2013). The second wave of digital-era governance: A quasi-paradigm for government on the Web. *Philosophical Transactions of the Royal Society A*,371(1987), 20120382.

Meijer, A. (2015). Government transparency in historical perspective: From the ancient regime to open data in the Netherlands. *International Journal of Public Administration*, 38(6), 393-414.

National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

Organization for Economic Co-operation and Development (OECD). (2020). *Digital government index: 2019 results*. OECD Publishing. https://doi.org/10.1787/4de9f5bb-en

Organization for Economic Co-operation and Development (OECD). (2021). *Model rules for reporting by platform operators with respect to sellers in the sharing and gig economy*. OECD Publishing. https://www.oecd.org/tax/exchange-of-tax-information/model-rules-for-reporting-by-platform-operators.htm

Phra Maha Thai Noi Yanmethi (Salang Sing), & Phra Silasak Sumetho (Boonthong). (2021). Adjusting government organizations to the era Digital government. *Thammasat Academic Journal*, 21(3), 291-299. https://so06.tci- thaijo.org/index.php/dhammathas/article/download/250572/170071

Prachat thammarat. (2020*). Introduction to international law*. Chulalongkorn University Press.

Suphanat Satcharatana. (2022). Adaptation of the Ministry of Foreign Affairs to become a digital government according to the framework of Thailand's Digital Government Development Plan 2020 - 2022 [Master's Thesis, Chulalongkorn university]. https://digital.car.chula.ac.th/cgi/viewcontent.cgi? article=9351&context=chulaetd

Siriporn Kaewpila, & Apinya Rodanan. (2020). Digital transformation of government organizations to increase capacity. Competitive ability. *Modern Management Journal*, 18(1), 16-21.

Somchai Homlaor. (2015). *Thai legal history*, Winychon Publishing House.

Worajet Phakharat. (2019). *Law and the justice process*, Winyuchon Publishing House. Westby,

J. R. (2020). *Legal frameworks for data protection: A global perspective on privacy laws*. Oxford University Press.

Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial intelligence and the public sector:

Applications and challenges. *International Journal of Public Administration*, 42(7), 596-615. https://doi.org/10.1080/01900692.2018.1498103

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs.