LEVERAGING THAI LAWS AND ARTIFICIAL INTELLIGENCE IN PUBLIC SERVICES: COMBATING KAKISTOSCRYPTOCRACY AND GOVERNMENTAL POWER MARKET-ING IN THE VU-CHAOS WORLD

Srirath GOHWONG[1]

1 Department of Political Science and Public Administration, Faculty of Social Sciences, Kasetsart University, Thailand; srirath.g@ku.th

ARTICLE HISTORY
Received: 22 November 2024 **Revised:** 1 December 2024 **Published:** 15 December 2024

ABSTRACT

The aim of this study was to investigate the strategic application of laws and artificial intelligence by the Thai government in tackling the issues related to kakistocracy and the marketing of governmental power. The research utilized documentary analysis techniques. Findings indicated that Thai legislation played a crucial role in alleviating the negative effects of kakistocracy and governmental power marketing by establishing a robust legal framework that promoted data protection, transparency, and accountability. Moreover, it regulated media, protected intellectual property, and addressed cybercrime and financial integrity. Following this, the Thai government could have used AI and legal rules to reduce the dangers of corrupt government and abuse of power by protecting personal data, increasing transparency, fighting misinformation, and improving governance with data-driven choices. Nevertheless, AI and Thai laws significantly hinder the effectiveness of governance.

Keywords: Thai Laws, Artificial Intelligence (AI), Public Services, Kakistoscryptocracy, Governmental Power Market-ing, VU-CHAOS world

CITATION INFORMATION: Gohwong, S. (2024). Leveraging Thai Laws and Artificial Intelligence in Public Services: Combating Kakistoscryptocracy and Governmental Power Market-ing in the VU-CHAOS world. *Procedia of Multidisciplinary Research, 2*(12), 4.

INTRODUCTION

In today's digital age, combining Thai laws with AI capabilities has become crucial for public services, especially when facing challenges from kakistoscryptocracy. This integration is vital because non-state actors (including tech giants like VK and Kaspersky Lab, non-government-based cryptocurrency users, and pirate organizations) can arbitrarily operate outside government control, potentially threatening national security and sovereignty. For example, when cybercriminals use Monero and its family (such as MoneroC, Monero Gold, MoneroV, Monero Classic, Monero-Classic, Monero 0, Monero Original) for illegal transactions, AI-powered systems can effectively help detect suspicious patterns while Thai cybercrime laws obviously provide the legal framework for prosecution. The effectiveness of this method arises from establishing a strong defense system that merges technology with legal frameworks to safeguard public interests. Nonetheless, this integration encounters considerable obstacles in the realm of VU-CHAOS. Although Thai laws are extensive, covering various fields such as cybersecurity and data protection, they may find it difficult to keep pace with swift technological changes. The implementation of market-ing strategies by the government to maintain its authority may conflict with traditional governance approaches. For example, although artificial intelligence can assist in monitoring threats on social media, achieving a balance between privacy rights as stipulated in the Personal Data Protection Act 2019 and the need for surveillance becomes increasingly challenging. Thus, to stay pertinent in this VU-CHAOS environment, Thailand needs to create innovative approaches that integrate law enforcement with technology, particularly AI (Gohwong, 2018, 2021, 2023; Jermsittiparsert et al., 2023). Hence, the purpose of this article is to explore how the Thai government strategically employs its laws and AI to lessen the negative effects caused by both kakistoscryptocracy and governmental power market-ing.

LITERATURE REVIEWS

Thai laws

According to Gohwong's study in 2021, Thai key laws could be categorized into specific groups, each tailored to address unique needs within the digital economy. This classification significantly clarified their role in promoting security, regulation, and fairness across public services. Data governance and information security legislation, including the Electronic Transactions Act 2001, Electronic Transactions Act (No. 2) 2008, Electronic Transactions Act (No. 3) 2019, Electronic Transactions Act (No. 4) 2019, Personal Data Protection Act 2019, Cybersecurity Act 2019, Digital Government Administration and Services Act 2019, and the Act on Electronic Means-based Public Service 2022, created a secure framework for the management of personal data. The regulations ensured the safety and availability of online healthcare and tax payments, while also increasing trust in online transactions. Yet, effectively enforcing these regulations may prove challenging given the rapid pace of technological advancements. Legislation targeting regulatory organizations, such as the Broadcasting and Television Businesses Act of 2008, the Telecommunications Business Act of 2001, and the Telecommunications Business Act (No. 2) of 2006, aimed to regulate competition and uphold standards within the telecommunications industry, which is crucial for dependable access to public digital services like online education. Nevertheless, overly strict regulations could stifle innovation, highlighting the need for a thoughtful approach to their enforcement. Then, laws centered on property rights, such as the Copyright Act 1994; Copyright Act (No. 2) 2015; Copyright Act (No. 3) 2015; Copyright Act (No. 4) 2018; Patent Act 1979; Patent Act (No. 2) 1992; Patent Act (No. 3) 1999; Trademark Act 1991; Trademark Act (No. 2) 2000; and Trademark Act (No. 3) 2016, were designed to safeguard intellectual property, thereby promoting innovation and supporting content creation, which was advantageous for public services like digital libraries. The current protective measures were designed to attract foreign

investment; however, the implementation of these measures could prove challenging, particularly due to concerns related to digital piracy. Then, laws like the Computer Crime Act of 2007 and the Computer Crime Act (No. 2) of 2017 tackled vital matters like cyber-attacks to safeguard digital public services. Although these regulations enhanced cybersecurity, facing difficulties in enforcing them on global cybercrimes was important to ensure that individuals' privacy rights were respected during their implementation. Public and private laws established a framework for governmental operations and private sector interactions, respectively. Furthermore, financial regulations, including the Currency Act of 1958, the Budgetary Procedures Act of 2018, the Fiscal Responsibility Act of 2018, and the Notification from the Director-General of the Revenue Department regarding Stamp Duty (Nos. 58 and 59) concerning cash payment methods for electronic transactions, alongside planning-related laws such as the Royal Decree on Criteria and Procedures for Good Governance of 2003 and its subsequent version in 2019, the National Strategies Preparation Act of 2017, the Royal Command on the National Strategy Announcement for 2018-2037, the National Reform Plans and Procedures Act of 2017, and the Royal Command regarding the Thirteen National Economic and Social Development Plan (2023-2027), were crucial for ensuring financial transparency and effective governance. Together, these legal classifications were essential to maintain a secure and efficient public service landscape in Thailand's digital economy (Currency Act 1958; Gohwong, 2021; Act on Electronic Means-based Public Service 2022, Royal Command Re: Announcement of Thirteen National Economic and Social Development Plan (2023-2027)).

Artificial Intelligence

Artificial intelligence (AI) was a field of study dedicated to developing computer systems that could perform tasks usually requiring human intelligence. These included language comprehension, image analysis, data-driven learning, and decision-making. Machine Learning (ML), a well-known branch of artificial intelligence, used algorithms that let computers learn and improve their performance through experience without explicit programming. Supervised learning (SL) was one of the different forms of machine learning, where AI learned from labeled examples. For example, it could spot instances of fraudulent government spending by highlighting unusual transactions. Unsupervised Learning (UL) sought to uncover hidden patterns in data without the use of labeled examples, as evidenced by the detection of misleading information on social media platforms. Semi-supervised learning (SSL) was beneficial in situations with limited information, like detecting corruption early, by utilizing a combination of small labeled data sets and abundant unlabeled data. Reinforcement learning (RL) was an alternative method for artificial intelligence to gain knowledge through interactions with the environment, like enhancing resource distribution during crises. These techniques enabled organizations, governments, and different sectors to make decisions that were better informed, quicker, and more transparent. Deep Learning (DL), a more sophisticated type of artificial intelligence, used neural networks to simulate the structure of the human brain. This progression enabled machines to collect insights from large data sets and recognize intricate patterns. Computer Vision (CV) was a domain dedicated to the analysis and processing of images or videos, and it represented just one of the many uses of deep learning. For example, it may have been used to monitor infrastructure projects and verify compliance with regulations. Natural Language Processing (NLP) improved AI's ability to understand and interpret human language, resulting in advancements in speech analysis as well (Banafa, 2024; Hemachandran & Rodriguez, 2024; Lucci et al., 2022; Shirkin, 2020).

Kakistoscryptocracy

Kakistoscryptocracy referred to a system characterized by the influence of powerful non-state entities, such as clandestine organizations, cryptocurrency users, and "net states"—which included major technology firms like VK, Yandex, Kaspersky Lab, Microsoft, Google, and

Facebook—that operated outside the purview of governmental authority, thereby undermining national sovereignty. This concept, introduced by Srirath Gohwong in 2023, highlighted a scenario in which these entities harnessed the deep web, dark web, non-governmental cryptocurrencies (NGCs), Web 3.0, and blockchain technology to conduct transactions without regulatory supervision. For example, pirate organizations or individuals might have used NGCs to avoid taxes or partake in illegal trade without state intervention. These unregulated actions created significant difficulties for governments, leading to a reduced ability to control various facets of law enforcement and financial regulation, which in turn eroded their power and influence in both the physical and digital arenas (Gohwong, 2020, 2023a, 2023b).

Governmental power market-ing in the VU-CHAOS world

Government power market-ing encompassed the application of market-ing techniques to reinforce and expand governmental authority over the populace. This approach integrated various tools, such as outreach programs, political messaging, and strategic initiatives, to shape public perceptions and behaviors. Authorities utilized methods like the promotion of social norms, emotional appeals, and the provision of incentives to garner support for particular policies or viewpoints, frequently with the objective of achieving lasting influence. An example would be if a government encouraged healthy habits and gained credibility by implementing public health initiatives. It also discussed gerontocracy—the influence of older generations in governance—which, although it brought continuity, could sometimes hinder innovation and adaptability to younger perspectives. Moreover, governing bodies also had to put in place control measures to maintain authority and assess how resources were obtained and used by the government to meet public needs. These strategies could have included utilizing data analytics tools to predict and mold public interest, along with political messaging to sway public opinion. In these frameworks, the concept of "market-ing of governmental power" was studied to grasp how power was spread and upheld among various sectors of society. This theory evaluated effectiveness based on factors like cost-benefit analysis, social impact, and demographic coverage (Jermsittiparsert, Gohwong, Pavapanunkul, Mahittichatkul, 2023).

RESEARCH METHODOLOGY

This study extensively utilized in-depth documentary analysis. The data were elaborately collected from diverse and up-to-date sources, encompassing books, peer-reviewed publications, and credible online resources.

RESEARCH RESULTS

Thai Laws' Role in Lessening the Negative Effects of Kakistoscryptocracy and Governmental Power Market-ing in the VU-CHAOS World

In the VU-CHAOS world, where volatility, uncertainty, complexity, and ambiguity disrupted traditional governance, Thai laws played a critical role in mitigating the negative effects of kakistoscryptocracy and governmental power market-ing. First, kakistoscryptocracy, a governance model where non-state actors evaded government oversight using decentralized technology, and governmental power market-ing, where governments manipulated public opinion to maintain control, both threatened state sovereignty. Thai laws (such as the Official Information Act 1997, Personal Data Protection Act 2019, Cybersecurity Act 2019, Digital Government Administration and Services Act 2019, and Act on Electronic Means-based Public Service 2022) created a legal framework to counter these threats by ensuring data protection and transparency. The data protection regulations prevented non-state actors from using digital data for illicit purposes, limited governmental interference, and created protections for personal information against unauthorized access. These laws required strict security measures to safeguard people's privacy rights and maintain a responsible digital environment in cases where dishonest people tried to obtain unauthorized access to citizens' data. Next, Thai

regulations governed media, communication platforms, and data handling to prevent monopolies and the dissemination of fake news. Multiple legislations, such as the Telecommunications Business Act of 2001, the Radio Communications Act of 1955, the Thai Public Broadcasting Service Act of 2008, and the Organization to Assign Radio Frequency and Regulate the Broadcasting and Telecommunications Services Act (No. 3) of 2019, existed to supervise media operations and guarantee equal access, visibility, and fairness in communication platforms. Implementing strict regulations on the media effectively prevented corrupt entities from taking control of information, thereby reducing the potential for government manipulation of public perception. Then, within the tumultuous VU-CHAOS setting, where uncontrolled media could sway public opinion, Thai legislation ensured the integrity of data, fostering an informed public that was less susceptible to manipulation. Key laws such as the Copyright Act (No. 4) of 2018, the Patent Act (No. 3) of 1999, and the Trademark Act (No. 3) of 2016 safeguarded intellectual property rights, curtailed monopolistic practices by large corporations, and encouraged equitable competition, all of which were vital for maintaining economic stability in a kakistocratic environment.

Moreover, to efficiently mitigate destabilizing impacts on economic and digital systems, Thai regulations emphasized the importance of financial transparency and the fight against cybercrime. The Computer Crime Act 2007 and Computer Crime Act (No. 2) 2017 directly empowered authorities to address cyber threats, fraud, and misinformation, allowing swift action against cyberterrorism and digital fraud, which were prevalent in kakistoscryptocracies. Then, public and administrative laws, such as the Constitution of the Kingdom of Thailand 2017 and Administrative-oriented laws (Administrative courts and administrative court procedure 1999), ensured accountability within governance by holding officials accountable and curtailing misuse of power. After that, financial regulations, including the Emergency Decree on the Digital Asset Businesses 2018 and Emergency Decree on the Amendment of the Revenue Code (No.19) 2018, maintained transparency in cryptocurrency transactions, protecting the economy from unregulated digital currencies often exploited by non-state actors to disrupt financial stability. Thai laws promoted economic stability by regulating virtual assets and digital currencies, thereby preventing non-state entities from manipulating markets for personal or political gain. Lastly, legislation focused on planning, including the Royal Decree on Criteria and Procedures for Good Governance 2003, the Royal Decree on Criteria and Procedures for Good Governance (No. 2) 2019, the Royal Command regarding the Announcement of the National Strategy 2018 - 2037, the National Reform Plans and Procedures Act 2017, and the Royal Command concerning the Announcement of the Thirteen National Economic and Social Development Plan (2023-2027), ensured that governance decisions prioritized long-term societal welfare over short-term gains. This method reduced the danger of power being centralized in corrupt organizations and promoted sustainable growth within the realm of worldwide digital changes. Overall, Thailand's extensive legal structures significantly reduced the chances of kakistocracy and power misuse, enabling the country to successfully handle and safeguard its activities in the tumultuous VU-CHAOS setting (Gohwong, 2020, 2021, 2023a, 2023b; Jermsittiparsert et al., 2023).

The Use of AI and Thai Laws in Lessening the Negative Effects of Kakistoscryptocracy and Governmental Power Market-ing in the VU-CHAOS World

In a world of VU-CHAOS, the Thai government utilized AI and legal structures to reduce the negative impacts of kakistoscryptocracy and the marketization of governmental power, as shown in Table 1. In order to address this issue, the Thai government could use Supervised Learning to examine corruption patterns in spending. These models, which were developed using historical data, would have been able to detect suspicious activities, alerting authorities to possible misuse before it could escalate. Backed by public legislation (including the Constitution of the Kingdom of Thailand 2017 and the Administrative Courts and

Administrative Court Procedure 1999), the Computer Crime Act 2007, and the Computer Crime Act (No. 2) 2017, AI could help the Thai government fulfill its legal commitments to data governance and anti-corruption initiatives, enforce accountability, and improve transparency. Next, the government could have utilized AI to combat false information and unethical tactics commonly seen in government propaganda efforts. Through the application of Unsupervised Learning and Natural Language Processing, AI could have examined extensive datasets from social media, news sources, and public forums to identify patterns of misinformation and propaganda techniques. This approach could have facilitated the proactive identification of coordinated disinformation campaigns that could distort public perception. The government could have meticulously regulated the media landscape through legislation such as the Telecommunications Business Act (No. 2) 2006, the Broadcasting and Television Businesses Act 2008, the Radio Communications Act 1992, and the Thai Public Broadcasting Service Act 2008. This could have fostered a public sentiment that was more resilient to manipulation and promoted freedom of expression.

Moreover, the government could have enhanced monitoring of infrastructure projects by utilizing computer vision technology to assess satellite and drone imagery. This approach could have simplified the detection of any indications of poor quality construction or unethical actions, ensuring that taxpayer money was used wisely, lawfully, and in line with rigorous quality criteria. Public laws such as the Constitution of the Kingdom of Thailand 2017 and the Administrative Courts and Administrative Court Procedure 1999 promoted openness and responsibility in public initiatives, while laws like the Copyright Act (No. 4) 2018 and Patent Act (No. 3) 1999 safeguarded intellectual property rights and promoted excellence. The integration of these laws was designed to guarantee the allocation of government resources towards high-quality, sustainable development, while simultaneously minimizing corruption and promoting the ethical application of computer vision in public infrastructure. Then, Semi-Supervised Learning could have assisted in monitoring government activities by analyzing patterns in incomplete documentation, potentially uncovering early signs of irregularities or corruption. The Official Information Act 1997 ensured that sensitive data was managed appropriately, with clear guidelines on permissible access and analysis for such tasks.

Lastly, the Thai government could have adopted strategies like Reinforcement Learning and Generative Learning to minimize mismanagement and improve governance in times of crisis. AI employing reinforcement learning could have made data-driven decisions, resulting in improved operational efficiency and equity. This approach could have assisted in optimizing resource distribution during emergencies. The Copyright Act of 1994, amended in 2015 and 2018, safeguarded government agencies' algorithms and other intellectual property from unauthorized use. At the same time, Generative Learning could have assessed different policy scenarios to uncover potential vulnerabilities that could be exploited. By implementing these AI methods within the strategic framework provided by the National Strategy 2018-2037 established by the Royal Command, which defined goals for sustainable governance, Thailand could have reduced the influence of short-term, self-serving incentives. This was achieved by embedding AI within regulatory structures and creating a governance model focused on stability and long-term planning (Banafa, 2024; Gohwong, 2020, 2021, 2023a, 2023b; Jermsittiparsert et al., 2023; Hemachandran & Rodriguez, 2024; Lucci et al., 2022; Shirkin, 2020).

Table 1 AI, Thai Laws, Kakistoscryptocracy and Governmental Power Market-ing

AI Technique	Application in Mitigating Negative Effects	Related Thai Laws
Supervised Learning	Predicts governance failures by analyzing corruption patterns	Public Laws, Computer Crime-Related Laws
Unsupervised Learning	Detects hidden patterns of misinformation or propaganda	Regulator-Oriented Laws, Data Governance & Information Security Laws
Semi-Supervised Learning	Identifies emerging threats with limited data	Data Governance & Information Security Laws
Reinforcement Learning	Optimizes decision-making in crisis scenarios	Planning-Oriented Laws, Money-Oriented Laws
Computer Vision	Monitors public infrastructure and detects fraud	Public Laws, Property Rights-Based Laws
Natural Language Processing	Analyzes legal texts and media for manipulation	Regulator-Oriented Laws, Public Laws
Generative Learning	Simulates policy outcomes to prevent exploitation	Planning-Oriented Laws, Property Rights-Based Laws

Source: Banafa (2024), Gohwong (2020, 2021, 2023a, 2023b), Jermsittiparsert et al. (2023), Hemachandran and Rodriguez (2024), Lucci et al. (2022), and Shirkin (2020)

DISCUSSION & CONCLUSION

The effectiveness of governance is notably undermined by the constraints posed by AI and Thai legal frameworks. A key limitation of AI stems from its dependence on abundant and high-quality data. AI systems, particularly those based on machine learning, require precise data to produce dependable predictions. When data is lacking or flawed, AI models can yield unreliable results, potentially worsening existing social inequalities. In the context of anti-corruption oversight, AI might overlook certain areas while disproportionately focusing on others due to biased data, resulting in a skewed perception of the corruption landscape. Furthermore, the incorporation of AI technologies requires considerable investment in terms of time, finances, and expertise. Sustaining these components can be expensive and challenging, especially for large government entities. Consequently, organizations might struggle to effectively manage and advance these technologies moving forward due to the substantial resource demands for AI projects in Thailand. Lastly, the effectiveness of Thailand's regulatory framework is further influenced by legal limitations. While Thai laws provide fundamental guidelines, they may lack the flexibility necessary to swiftly respond to emerging technological challenges or to satisfy the changing governance demands within the VU-CHAOS context. Moreover, if enforcement measures are not consistently enforced, legislation concerning transparency and data protection may not effectively stop unauthorized individuals from accessing government data, which could lead to an increase in corruption. However, excessive restriction could have limited technological advancement in AI. Therefore, the Thai government faces a delicate balance in regulating AI applications to mitigate risks while promoting technological growth in public administration.

REFERENCES

Banafa, A. (2024). *Introduction to Artificial Intelligence (AI)*. River Publishers.

Gohwong, S. (2018). *The state of the art of privacy-oriented cryptocurrencies*. 5th International Social Sciences and Business Research Conference, Università della Svizzera italiana Lugano, Switzerland, 30 May 2018.

Gohwong, S. (2020). *Net States and their roles in Russia*. Paper presented at the 7th International Conference on Security Studies, Town in Town Hotel, Bangkok, Thailand, 23 July 2020.

Gohwong, S. (2021). The state of the art of key public service provision-related laws under digital economy in Thailand. *Psychology and Education Journal, 58*(3).

Gohwong, S. (May 9, 2023a). Kakistoscryptocracy. *Asian Political Science Review, 7*(1), 50-58.

Gohwong, S. (2023b). Russian Net States and Their Roles in Russia. *Procedia of Multidisciplinary Research, 1*(11), 11.

Jermsittiparsert, K., Gohwong, S., Pavapanunkul, S., Mahittichatkul, N. (2023). *Governmental power market-ing in the VU-CHAOS world*. PA: IGI Global.

Hemachandran, K., & Rodriguez, R. V. (2024). *Artificial Intelligence for Business: An Implementation Guide Containing Practical and Industry-Specific Case Studies*. Routledge.

Lucci, S., Musa, S. M., & Kopec, D. (2022). *Artificial Intelligence in the 21st Century*. Mercury Learning and Information.

Shirkin, R. (2020). *Artificial Intelligence: The Complete Beginners' Guide to Artificial Intelligence*. Amazon KDP Printing and Publishing.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Conflicts of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.