International Journal of Development Administration Research

Criminal Law Enforcement and Penal Sanctions for the Illegal Sale of Personal Data in Thailand

Vichan Chanin[1] Kajornatthapol Pongwiritthon[2*] Suttipong Thumtheang[3] and
Chavalit Honglertsakul[4]
Faculty of Law and Political Science, Northern College, Thailand.[1]
Faculty of Business Administration, Northern College, Thailand,
IQRA Business School, University of Geomatika Malaysia.[2*]
Doctor of Medicine Boston University, USA, Entrepreneurs of IDE Clinic.[3]
Division of Urology, Department of Medicine, Faculty of Medicine, Vajira Hospital, Navamindhradiraj University.[4]
Corresponding Author Email: tok2029@gmail.com

Received: November 06, 2025	Revised: December 30, 2025	Accepted: December 31, 2025

Abstract

This research examines the adequacy of Thailand’s legal framework in deterring and sanctioning the illegal sale of personal data, with particular attention to enforcement under the Personal Data Protection Act B.E. 2562 (PDPA). Using a qualitative documentary approach grounded in legal hermeneutics, the study analyzes statutory provisions, doctrinal writings, and comparative legal standards to evaluate whether current sanctions achieve proportionality and deterrence in the context of cross-border and technology-driven data markets. The findings reveal a critical loophole: Section 80 of the PDPA imposes criminal liability primarily on state officials, thereby excluding private individuals and non-state actors—who constitute a major source of unlawful data trading—from direct criminal accountability. In addition, the penalties available under relevant Thai laws are comparatively mild when benchmarked against international standards, where regimes such as the GDPR and the UK Data Protection Act 2018 authorize significantly higher financial sanctions and more robust enforcement mechanisms. The hermeneutic method is particularly suited to this inquiry because it enables interpretation of legislative intent, structural gaps, and practical enforceability across intersecting legal instruments, addressing jurisdictional complexity and evidentiary barriers that cannot be resolved through purely textual comparison of statutes. Based on these findings, the study proposes legal reforms including the expansion of criminal liability to private actors, clearer definitional elements of "unlawful data sale," and a tiered sanction model designed to strengthen deterrence while preventing over-criminalization. These reforms aim to align Thai enforcement capacity with the realities of contemporary personal data trafficking and transnational digital crime.

Keywords: Personal Data Protection Act (PDPA), Unlawful Data Sale, Criminal Liability of Private Actors, Legal Hermeneutics

Introduction

In the contemporary digital era, rapid technological advancement and the widespread use of digital platforms have elevated personal data protection to a global priority. The increasing exchange of personal information through online channels and smart devices has created a critical need for effective legal mechanisms to safeguard individual privacy. Beyond its economic value, personal data is increasingly recognized as a component of individual autonomy and dignity, reflecting the principle of **informational self-determination**, which emphasizes a person's right to control the collection, use, and disclosure of information about themselves. When personal data is unlawfully accessed or traded, the harm extends beyond technical security failures and may result in identity theft, fraud, and reputational harm. These risks ultimately undermine public trust in digital services and erode the legal foundations required for sustainable digital economic growth. To mitigate such harms, many countries have enacted comprehensive data protection laws aimed at safeguarding citizens' rights and privacy.

The European Union's General Data Protection Regulation (GDPR), which came into effect in 2018, serves as one of the most influential models of data protection law, imposing strict compliance obligations on organizations that process personal data and establishing significant administrative fines for violations (Wolford, 2024). Similarly, in the United States, California pioneered the California Consumer Privacy Act (CCPA) in 2020, granting consumers enhanced control over their personal information (State of California Department of Justice, 2024). In the United Kingdom, the Data Protection Act 2018 sets out core principles for lawful and transparent processing while prescribing criminal sanctions for non-compliance (legislation.gov.uk, 2024). Collectively, these legal frameworks reflect the recognition that personal data protection constitutes a fundamental right grounded in human dignity and individual autonomy, while also functioning as a governance tool necessary for effective regulation of digital markets and illicit data economies.

Thailand's awareness of personal data protection emerged alongside the country's accelerated digital transformation. The Personal Data Protection Act B.E. 2562 (2019), which came into full effect on June 1, 2022, represents Thailand's first comprehensive legislation dedicated to protecting individual privacy rights. The Act establishes clear standards for data collection, usage, disclosure, transfer, and deletion, requiring data controllers to maintain appropriate security measures and inform data subjects about the purposes, retention periods, and rights regarding their data (Office of the Personal Data Protection Committee, 2024). Violations of the PDPA may result in administrative fines of up to five million baht or imprisonment for up to one year, or both (BBC News Thai, 2024). Consequently, both businesses and individuals are legally obligated to comply with the PDPA to ensure responsible data governance. However, the effectiveness of a legal regime in addressing illicit data markets depends not only on compliance standards and administrative enforcement, but also on whether the legal system can impose meaningful deterrence against intentional and profit-driven wrongdoing, particularly where personal data is commodified and trafficked.

Personal data has increasingly become a high-value asset. Public and private sectors actively seek to collect, analyze, and utilize personal information for business planning and targeted marketing (Rattanapornsuwan, 2023). However, this demand has also encouraged the illicit trade of personal data, resulting in widespread violations of privacy rights. The United Nations Human Rights Council (2018) reported that the global market for illegally traded personal data exceeds three billion U.S. dollars annually. In Thailand, the issue has intensified in recent years. The Office of the Personal Data Protection Committee (2024a) recorded 432 complaints related to data privacy violations between 2021 and 2024, along with 39 cases of illegal data sales and over 5,000 data leak incidents (Office of the Personal Data Protection Committee, 2024). Importantly, these figures do not merely indicate the prevalence of privacy violations; they also reveal persistent **enforcement challenges** within the national data protection system, including the scale and speed of incidents, the difficulty of attributing responsibility in complex data ecosystems, and the increasing involvement of private actors in the commodification and distribution of personal information. These violations undermine constitutional privacy rights enshrined in Section 32 of the Constitution of the Kingdom of Thailand B.E. 2560 (2017) and inflict economic and psychological harm, including financial losses from fraud, reputational damage, and emotional distress. Victims often face costly legal proceedings when seeking redress (Khamsom, Areerat, & Lekdee, 2024).

Despite the PDPA's enactment, Thailand's current legal framework lacks specific criminal provisions to address the illegal sale of personal data. The Constitution affirms privacy as a protected right, and the PDPA operationalizes this protection through regulatory duties and administrative sanctions. Nonetheless, when personal data is intentionally traded for unlawful gain, the harm resembles forms of economic and social wrongdoing traditionally addressed through criminal law. The legitimacy of criminal intervention can be explained through the state's **jus puniendi**, which authorizes penal sanctions where necessary to protect fundamental rights and uphold public order. In this context, reliance solely on administrative fines may be insufficient to deter private data traffickers who profit from unlawful data trading and can evade accountability through anonymity, intermediaries, and cross-border operations.

Section 80 of the Act criminalizes the unauthorized disclosure of personal data by officials performing duties under the Act, punishable by up to six months' imprisonment or a fine of 500,000 baht. However, the provision narrowly applies only to officials, excluding private individuals who engage in data trading for unlawful gain. This limitation has resulted in enforcement challenges and a lack of deterrence. Scholars and practitioners have argued that Thailand's existing legal measures emphasize civil penalties over criminal sanctions, leaving regulatory agencies without effective criminal enforcement tools (Royal Thai Government Gazette, 2019; Wipulakhom & Pitiyasak, 2021). In practice, this legal gap becomes more significant when incidents occur at scale, as suggested by the growing number of complaints and leak incidents, because the absence of direct criminal liability for private actors restricts investigative leverage and reduces the expressive and deterrent functions of criminal law.

Moreover, the cross-border nature of digital data transfer further complicates enforcement. Illicit actors often exploit jurisdictional loopholes by operating across multiple countries, making prosecution difficult. In contrast, international jurisdictions such as the United Kingdom, under Section 170 of the Data Protection Act 2018, provide explicit criminal sanctions for the unlawful sale of personal data. The United States has also established Data Protection

Authorities (DPAs) empowered to investigate, impose fines, and pursue litigation against violators while promoting public awareness about data privacy risks. These examples illustrate that effective data governance increasingly requires integrated enforcement that combines administrative, civil, and criminal mechanisms, particularly for intentional misconduct involving illicit data markets.

Given these limitations, Thailand's current legal framework remains insufficient to effectively prevent and penalize illegal data trading. The absence of a dedicated criminal provision leaves a regulatory gap that undermines the protection of citizens' privacy and the integrity of the country's digital economy. Strengthening criminal law enforcement through explicit penal sanctions is therefore essential to deter unlawful data transactions, protect citizens' fundamental rights, and enhance public confidence in the country's data governance regime.

This study titled "Criminal Law Enforcement and Penal Sanctions for the Illegal Sale of Personal Data in Thailand" is conducted to examine and analyze, (1) the conceptual and theoretical foundations of criminal penalties concerning the unlawful sale of personal data; (2) the challenges in enforcing criminal sanctions under existing Thai legislation; and (3) practical legal reform measures that could enhance Thailand's ability to prevent and suppress data-related offenses. By examining relevant provisions under the UK Data Protection Act 2018, Thailand's Personal Data Protection Act B.E. 2562 (2019), and the Computer Crimes Act B.E. 2550 (2007) and its amendments, this research aims to propose specific legislative reforms that would establish clear criminal liability for individuals or entities engaged in the illegal trade of personal data. The study ultimately seeks to provide legal and policy recommendations to strengthen Thailand's capacity to safeguard personal information, promote accountability, and ensure alignment with global standards for data protection and digital rights.

Objectives of Research

1. Examine the key concepts, theories, and legal principles governing criminal penalties for the unlawful sale of personal data.

2. Critically analyze the proportionality and deterrence of existing criminal sanctions under Thailand's Personal Data Protection Act B.E. 2562 (2019) and related laws, including the practical challenges of enforcement against unlawful personal data trading.

3. Analyze the jurisdictional overlap and enforcement tensions between the Personal Data Protection Act B.E. 2562 (2019) and the Computer Crimes Act B.E. 2550 (2007) and its amendments, particularly in cross-border and technology-enabled data trading contexts.

4. Propose legal and policy measures to improve the criminal penalty framework and strengthen protection against illegal data trading.

Research Methodology

This study investigates the enforcement of criminal law and the determination of penal sanctions concerning the unlawful sale of personal data in Thailand. It aims to examine the adequacy of existing legislation, identify gaps in criminal enforcement, and propose appropriate legal and policy recommendations. The analysis is grounded in both Thai and international legal frameworks, focusing on the Constitution of the Kingdom of Thailand B.E. 2560 (2017), the Criminal Code B.E. 2499 (1956), and the Personal Data Protection Act B.E. 2562 (2019), together with related ministerial regulations and administrative guidelines. Comparative studies of foreign legal systems, including those of the European Union and the United Kingdom, were conducted to provide broader perspectives on the imposition of criminal sanctions for unlawful data trading and to identify effective policy models adaptable to Thailand's context.

1. Research Design. A qualitative research design was employed using the documentary research method, a well-established approach in legal and policy studies. This method involves systematically collecting, interpreting, and synthesizing information from both primary and secondary legal sources to form a coherent analytical framework. According to Creswell and Poth (2018), qualitative inquiry allows for in-depth understanding of complex social and legal phenomena, particularly where human interpretation, ethics, and institutional structures intersect. The qualitative approach was selected because it provides flexibility in analyzing legal doctrines, judicial interpretations, and regulatory practices that cannot be captured through quantitative methods. By focusing on legal texts and interpretative reasoning, this method supports a nuanced examination of how criminal sanctions function in practice within Thailand's data protection regime. It also facilitates comparative evaluation with international legal systems, helping to formulate evidence-based and context-sensitive policy recommendations.

2. Theoretical and Legal Framework. The study is grounded in criminal law and criminological theories that explain the purposes and limitations of punishment. As Hart (1968) observes, criminal sanctions serve to uphold justice by balancing retribution, deterrence, and rehabilitation. These dimensions are particularly relevant to cyber-related crimes, where violations often cause intangible yet far-reaching harm to individuals and society. Thai criminal law is guided by the principles of legality, proportionality, and culpability, which together ensure that punishment is fair, just, and reflective of the offender's intent. These principles are embedded in the Criminal Code B.E. 2499 (1956) and further reinforced by the Personal Data Protection Act B.E. 2562 (2019) (Royal Thai Government Gazette, 2019). However, unlike comparable legal systems, Thailand's data protection law places greater emphasis on civil and administrative remedies, offering limited criminal enforcement provisions. In contrast, the European Union's General Data Protection Regulation (GDPR) (2016) and the United Kingdom's Data Protection Act 2018 establish explicit criminal penalties for unlawful data processing and sale, thereby strengthening accountability among data controllers and processors (Wolford, 2024; legislation.gov.uk, 2024). These comparative models illustrate how proportionate criminal sanctions can enhance deterrence while ensuring justice and fairness in enforcement.

3. Sources of Data. Primary data were obtained from Thai legal documents, including the Constitution of the Kingdom of Thailand B.E. 2560 (2017), the Criminal Code B.E. 2499 (1956), and the Personal Data Protection Act B.E. 2562 (2019), as well as related ministerial regulations and government publications. Additional information was collected from reports and announcements issued by the Personal Data Protection Committee (PDPC) and the Ministry of Digital Economy and Society. Secondary data included academic journals indexed in the Thai Citation Index (TCI) and Scopus, legal commentaries, research articles, theses, and conference proceedings relevant to data protection, cyber law, and criminal justice. International data sources such as the United Nations Human Rights Council Report (2018) on illicit data trading were also analyzed to contextualize global trends in criminal data enforcement. This multi-source approach ensured comprehensive and balanced insights that integrate both domestic and comparative perspectives.

4. Data Collection and Analysis. Data collection focused on identifying relevant legal provisions, enforcement practices, and jurisprudence addressing criminal liability in personal data protection. Key themes included (1) theoretical foundations of criminal sanctions, (2) enforcement mechanisms within the Thai legal framework, and (3) comparative perspectives from foreign jurisdictions. A qualitative content analysis approach was applied to interpret and evaluate the data. This technique emphasizes analytical depth and contextual interpretation over statistical generalization. Following the framework of Miles, Huberman, and Saldaña (2019), the analytical process comprised three stages: (1) Data Reduction, filtering and organizing legal materials to identify pertinent statutes, principles, and precedents; (2) Data Display, synthesizing findings through comparative tables and thematic summaries to visualize relationships among key legal issues; and (3) Conclusion Drawing and Verification, interpreting findings to propose recommendations for improving criminal law enforcement and ensuring alignment with international standards. Through this systematic process, patterns, inconsistencies, and legal ambiguities were identified and analyzed to clarify the limitations of current legislation and enforcement procedures in Thailand.

5. Challenges in Legal Enforcement. Despite the existence of the Personal Data Protection Act B.E. 2562 (2019), significant enforcement challenges remain. These include the absence of specialized investigative bodies, limited expertise in digital forensics, and jurisdictional complexities arising from cross-border data flows (United Nations, 2018). Furthermore, Thai law lacks a precise legal definition of "unlawful data sale," complicating criminal prosecution. Khamsom, Areerat, & Lekdee (2024) emphasize that effective deterrence requires enhanced inter-agency collaboration, the development of cybercrime-specific enforcement units, and the integration of forensic evidence into legal proceedings. Addressing these challenges requires a coordinated policy response that combines criminal law reform, institutional capacity building, and public awareness initiatives. Comparative analysis indicates that countries with well-defined legal frameworks and empowered regulatory agencies achieve higher compliance and deterrence outcomes.

6. Scope of the Study and Comparative Jurisdictions. The research scope covers both domestic and international legal contexts. Domestically, the study focuses on Thailand's Personal

Data Protection Act B.E. 2562 (2019), its criminal implications, and related administrative regulations. Internationally, it analyzes the enforcement mechanisms under the EU's GDPR and the UK's Data Protection Act 2018, as well as best practices in data protection governance. The comparative focus on the European Union and the United Kingdom is justified because these jurisdictions represent globally recognized benchmarks for mature data governance frameworks, including robust enforcement mechanisms and explicit criminal provisions for unlawful personal data processing and disclosure (Wolford, 2024; legislation.gov.uk, 2024). In addition, the study references the United States particularly through the development of consumer privacy protections such as the CCPA as a leading example of a large-scale digital economy that employs enforcement tools combining regulatory oversight and litigation-driven accountability (State of California Department of Justice, 2024). These jurisdictions provide useful comparative insights for strengthening Thailand's enforcement capacity and sanction design. Although other ASEAN neighbors may offer valuable localized perspectives, they were not selected as primary comparative cases in this study because the research objective emphasizes identifying **high-enforcement benchmark models** with established sanction structures that can inform reform proposals for Thailand. Moreover, ASEAN data protection regimes remain diverse in legal maturity and sanction mechanisms, which may limit direct comparability when the study's focus is the design and proportionality of criminal sanctions within a comprehensive enforcement framework. Nonetheless, ASEAN comparative analysis remains a valuable direction for future research, particularly for harmonization efforts and cross-border cooperation in regional data governance.

7. Research Limitations. This study adopts a documentary research approach that relies on statutes, official documents, and scholarly analysis. While this method provides systematic insight into legal structure, intent, and doctrinal consistency, it has limitations in capturing rapidly evolving technological practices. In digital law research, technological developments may outpace legislative reform, creating a moving target for regulatory responses. In particular, illicit personal data trading increasingly occurs through complex online ecosystems, including encrypted communication channels and anonymous marketplaces often associated with the "Dark Web." Such anonymity and transnational dispersion can constrain the practical applicability of reforms derived primarily from documentary analysis, especially where enforcement depends on real-time investigative capabilities, digital forensics, and cross-border cooperation. Furthermore, because documentary research prioritizes legal texts and publicly available sources, it may not fully reflect hidden practices of data brokers, underground market dynamics, or enforcement barriers encountered in active criminal investigations. As a result, the reform proposals in this study should be interpreted as **normative and structural recommendations** aimed at improving Thailand's legal framework and sanction design, while acknowledging that effective implementation requires parallel institutional development, technical capacity building, and inter-agency coordination (United Nations, 2018; Khamsom, Areerat, & Lekdee, 2024). Finally, although the study includes comparative benchmarks from jurisdictions with strong enforcement frameworks, the exclusion of ASEAN neighbors limits the extent to which regional legal convergence and localized enforcement practices are examined. Future research may expand the comparative scope to include ASEAN jurisdictions to strengthen regional contextualization and support cross-border policy harmonization.

Research Results

1) Issues in the Enforcement of Criminal Law on the Unlawful Sale of Personal Data. The study found that Thailand's Personal Data Protection Act B.E. 2562 (PDPA) establishes a foundational framework for protecting individual rights concerning the collection, use, and disclosure of personal data. However, the enforcement of Section 80, which criminalizes the unauthorized disclosure of personal data by officials, remains limited in scope and effectiveness. The provision applies only to officials who access personal data in the course of their duties and does not extend to private individuals engaged in the unlawful sale or trafficking of personal data. This exclusion creates a significant legal loophole and weakens criminal accountability in real-world data markets, where private actors frequently play a central role in commodifying and distributing personal data for profit (Khamsom, Areerat, & Lekdee, 2024). In practice, Thailand's enforcement is constrained by structural and procedural limitations. State agencies lack adequate criminal mechanisms to investigate and prosecute personal data trafficking effectively, particularly where offenses occur through transnational networks and anonymous online environments. These constraints are compounded by the complexity of digital evidence collection, attribution challenges (identifying the true perpetrator behind accounts or intermediaries), and jurisdictional limitations when offenders operate across borders (United Nations, 2018). As a result, enforcement tends to be reactive, fragmented, and insufficiently deterrent, especially against organized and profit-driven data trading. By comparison, international jurisdictions demonstrate broader criminal coverage and stronger enforcement models. In the United States, the California Consumer Privacy Act (CCPA) provides consumers with legal rights to sue companies for data breaches and unauthorized data use. Under Section 1798.150(b), businesses are provided 30 days to cure violations before facing legal action, balancing deterrence with compliance (State of California Department of Justice, Office of the Attorney General, 2024). At the federal level, the Computer Fraud and Abuse Act (CFAA) criminalizes unauthorized access to computer systems, with penalties of up to ten years' imprisonment (U.S. Department of Justice, 2022). In the United Kingdom, Section 170 of the Data Protection Act 2018 explicitly criminalizes the obtaining, disclosure, and sale of personal data obtained unlawfully, regardless of the actor's official capacity (ICO, 2023). The Information Commissioner's Office (ICO) also has direct investigative and prosecutorial functions, supporting more effective enforcement. These comparative frameworks collectively reinforce that criminal sanctions must extend to private actors and be supported by enforceable investigative authority to deter illicit data markets effectively.

2) Legal Characterization of Offenses by Private Individuals. A central finding is that the absence of explicit provisions addressing the unlawful sale of personal data by private individuals constitutes a major weakness in Thai law. Section 80 of the PDPA applies narrowly to persons acting in an official or authorized capacity and does not clearly encompass private citizens who intentionally buy, sell, or broker personal data. This limitation obstructs the criminalization of conduct that poses significant risks to privacy rights and national cybersecurity, particularly when personal data is trafficked as a commodity across online networks (Suraratchai, 2023). In contrast, under the UK DPA 2018, private individuals who unlawfully obtain, disclose, or sell personal data may face up to five years' imprisonment or an unlimited fine (ICO, 2023). The comparative insight underscores an important doctrinal issue: the Thai framework does not provide sufficiently clear definitional elements for "unlawful data sale," creating uncertainty in determining whether private data transactions constitute crimes. This ambiguity undermines deterrence and conflicts with the criminal law principle of legality, which requires clear and specific definitions of punishable conduct (Hart, 1968). From a human rights perspective, this gap also conflicts with the right to informational self-determination and the protection against unlawful interference with privacy recognized under Article 17 of the ICCPR. Therefore, the study concludes that reform must explicitly extend criminal liability to individuals and entities engaged in intentional personal data trading or profiteering, while specifying offense elements such as unlawful acquisition, intent to trade, and knowledge (or reckless disregard) regarding illegality.

3) Penalties and Liability for Illegal Data Trading on Online Platforms and Dark Web Markets. The study further finds that the PDPA (2019) and the Computer Crime Act (2007, amended 2017) collectively regulate certain categories of data misuse and cyber offenses, yet both fail to address the commercialized trading of personal data by private actors on online platforms and anonymous markets. The Computer Crime Act primarily targets false data insertion, unauthorized access, and technology-facilitated harms, whereas the PDPA focuses on improper disclosure by authorized persons. Consequently, neither statute provides direct criminal liability for private actors who advertise, broker, or sell personal data as a commodity online (Suraratchai, 2023). More granularly, illicit data trading increasingly occurs through multi-layered online environments that include (1) open social media channels and messaging platforms where data lists may be advertised or exchanged; (2) semi-private groups with controlled membership where data is offered to buyers; and (3) Dark Web marketplaces where stolen records are sold using encryption, anonymizing technologies, and cryptocurrency payment mechanisms. These ecosystems are designed to obscure identity and jurisdiction, creating substantial barriers to detection, evidence collection, and prosecution (Anderson et al., 2021). Even where a data leak is detected, linking the leaked dataset to the original unauthorized access and proving the chain of distribution can be difficult, especially when perpetrators rely on intermediaries or cross-border infrastructure (United Nations, 2018). Accordingly, the results suggest that Thai law must move beyond targeting “false data” or internal unauthorized disclosure and explicitly criminalize: (1) the sale, exchange, or distribution of personal data obtained unlawfully; (2) the intentional facilitation or hosting of such transactions on digital platforms; and (3) the use of unlawfully obtained personal data for fraud or profit-seeking purposes (Suraratchai, 2023; Anderson et al., 2021). The study also finds that institutional limitations particularly digital forensic capacity and coordination significantly hinder enforcement, indicating that legal reform should be accompanied by stronger inter-agency mechanisms and investigative capability (United Nations, 2018).

4) Comparative "Data Display": Key Legal Gaps Between Thailand, the UK, and the GDPR. Consistent with the study's methodology (Miles, Huberman, & Saldaña, 2019), the results are summarized through a comparative table to highlight structural gaps in Thai enforcement compared with the UK and EU benchmarks. As shown in Table 1.

Table 1. Comparative Gaps in Criminal Coverage and Sanctions (Thailand vs UK DPA 2018 vs GDPR)

Dimension	Thailand: PDPA (Section 80)	UK: DPA 2018 (Section 170)	EU: GDPR (Article 83)
Who is criminally liable?	Primarily officials performing duties under the Act	Any person (including private individuals)	Primarily administrative liability for controllers/processors; criminalization left to member states
Core prohibited conduct	Unauthorized disclosure by officials	Unlawful obtaining, disclosure, or sale of personal data	Violations of processing obligations; broad compliance duties
Coverage of private data trading	Not explicit; major loophole	Explicitly criminalized	Not directly criminalized at EU level; addressed through fines/regulatory enforcement
Maximum sanction severity	Relatively limited imprisonment/fine	Up to five years' imprisonment or unlimited fine	Administrative fines up to €20 million or 4% of global turnover
Deterrence mechanism	Limited economic deterrence due to low penalty ceiling	Stronger deterrence through criminal liability + severe sanctions	Strong economic deterrence through high-scale administrative fines
Enforcement authority	PDPC has limited prosecutorial authority	ICO has investigative/prosecutorial functions	Supervisory authorities with strong enforcement powers

(ICO, 2023; European Union, 2016; Wolford, 2024; Royal Thai Government Gazette, 2019)

This table 1. supports the key conclusion that Thailand's legal gap is not merely about the "amount" of penalties, but also about the scope of liability (exclusion of private actors), the absence of explicit criminalization of trading conduct, and the limited enforcement architecture.

5) Proportionality and Adequacy of Criminal Sanctions: The Case for a Tiered Sanction Structure. The results show that current penalties under Section 80 of the PDPA imprisonment for up to one year or a fine not exceeding 1 million THB are disproportionate to the financial gains obtained from unlawful personal data trading. Such penalties fail to generate adequate deterrence, especially when personal data trafficking yields high profits and can be repeated at scale. By contrast, the UK DPA 2018 imposes up to five years' imprisonment or unlimited fines (ICO, 2023), and international practice demonstrates the importance of economic deterrence through sanctions that exceed potential gains. A key comparative illustration is the Facebook case (2019), where the company was fined USD 5 billion for data privacy violations, underscoring how large-scale sanctions operate as a deterrent where misconduct produces significant economic benefit (United Nations Human Rights Council, 2018). Based on this finding, the study argues that Thailand should adopt a tiered sanction structure that differentiates sanction levels based on: (1) offender intent (willful, reckless, negligent); (2) scale, volume, and sensitivity of data involved; and (3) demonstrable harm to data subjects and public confidence. Such a model would strengthen deterrence while preserving proportionality, ensuring that sanctions do not unduly penalize organizations involved in unintentional or non-malicious incidents. In addition, granting the Personal Data Protection Committee (PDPC) greater procedural authority to initiate criminal proceedings—similar to the UK's ICO—would enhance enforcement efficiency. The establishment of a specialized Cyber Data Protection Taskforce would further streamline investigations and strengthen cross-agency cooperation (United Nations, 2018; Khamsom, Areerat, & Lekdee, 2024). From a human rights perspective, strengthening sanctions aligns with Thailand's obligations under the UDHR and ICCPR to protect citizens' privacy against unlawful interference.

6) Summary of Key Findings. The findings reveal that Thailand's Personal Data Protection Act B.E. 2562 represents significant progress in data governance but remains limited in criminal enforcement scope. The main issues include: (1) Narrow applicability of Section 80, which excludes private individuals from liability; (2) Insufficient penalties that fail to deter lucrative data trading schemes; (3) Weak institutional enforcement due to the PDPC's limited prosecutorial authority; and (4) Absence of effective cross-border cooperation mechanisms, impeding investigation of transnational offenses. Comparative analysis with the DPA 2018, GDPR, CFAA, and CCPA demonstrates that a multi-layered enforcement structure combining administrative, civil, and criminal mechanisms is essential for effective deterrence. Reforming Thailand's PDPA to expand criminal scope, increase proportional sanctions, and strengthen PDPC authority would bridge current gaps and align the country's data protection system with international best practices (European Union, 2016; ICO, 2023; U.S. Department of Justice, 2022; State of California Department of Justice, Office of the Attorney General, 2024).

Discussion of Research Results

This study examined criminal-law enforcement and penal sanctions for the unlawful sale of personal data, with attention to (1) theoretical bases for punishment, (2) enforcement gaps in Thailand, and (3) avenues for legal and institutional reform. Overall, the findings show that Thailand's Personal Data Protection Act B.E. 2562 (PDPA) establishes a modern privacy framework but leaves decisive criminal-law gaps that weaken deterrence in digital markets for illicit data.

First, the results support the relevance of classic punishment rationales legality, proportionality, deterrence, and rehabilitation to data-crime contexts (Hart, 1968). Illicit data trade produces diffuse yet substantial harms (identity theft, fraud facilitation, and chilling effects on privacy), which justifies targeted criminalization in addition to administrative fines. However, proportionality requires calibrated sanctions that scale with the sensitivity, volume, and downstream exploitation of personal data. The current Thai regime does not yet meet that calibration standard consistently, particularly where penalties are lower than the gains available from data trafficking (Suraratchai, 2023). This "penalty–profit mismatch" undermines deterrence and may incentivize repeat offending in platform-mediated and cross-border environments (United Nations, 2018).

Second, comparative analysis clarifies how leading jurisdictions embed criminal accountability within broader data-protection systems. The United Kingdom's Data Protection Act 2018 (DPA 2018) criminalizes obtaining, disclosing, or selling personal data without authorization (s.170), and authorizes robust investigation and prosecution by the Information Commissioner's

Office (ICO), producing a credible threat of enforcement against both organizations and private actors (Royal Thai Government Gazette, 2019; legislation.gov.uk, 2024). In the European Union, the General Data Protection Regulation (GDPR) relies chiefly on administrative fines but is complemented in several member states by criminal provisions for aggravated conduct (European Union, 2016). In the United States, while privacy law is sectoral, a layered architecture private rights of action under the California Consumer Privacy Act (CCPA) and felony-level penalties under the Computer Fraud and Abuse Act (CFAA) for unauthorized access creates multiple enforcement levers that reach both companies and individuals (State of California Department of Justice, Office of the Attorney General, 2024). These models illustrate how criminal rules can be narrowly drawn yet effective when paired with specialized investigative powers and institutional capacity.

Third, the Thai findings highlight three structural enforcement obstacles. (1) Narrow offense coverage: PDPA Section 80 focuses on officials who unlawfully disclose data in the course of duty; it does not clearly capture private individuals who buy or sell personal data for gain. This leaves a "grey zone" for dark-market transactions and platform-mediated brokering (Rattanapornsuwan, 2023). (2) Evidence and jurisdiction: Investigating data trafficking requires digital forensics, chain-of-custody procedures, and cross-border cooperation; without these, prosecutions are slow or infeasible (United Nations, 2018). (3) Penalty–profit mismatch: Maximum custodial terms and fines under current provisions are often lower than the illicit profits available in underground markets, eroding deterrence and public trust (Suraratchai, 2023).

Fourth, the discussion supports reforms consistent with legality and proportionality. Substantively, the PDPA should be amended to: (a) define unlawful sale, exchange, brokerage, or distribution of personal data as distinct offenses applicable to any person; (b) recognize aggravating factors (e.g., large-scale datasets, vulnerable data such as health/biometric records, or sales to organized groups); and (c) adopt tiered penalties that scale with harm and intent, aligning with DPA 2018's approach (Royal Thai Government Gazette, 2019; legislation.gov.uk, 2024). Procedurally, enforcement would be strengthened by: (i) granting the Personal Data Protection Committee (PDPC) explicit powers to initiate criminal complaints and coordinate with the Technology Crime Suppression Division; (ii) formalizing digital-forensics standards; and (iii) establishing mutual legal assistance templates tailored to data-crime investigations. Complementary civil tools such as limited private rights of action for data subjects modeled on

CCPA could shift incentives toward prevention without over-criminalization (State of California Department of Justice, Office of the Attorney General, 2024).

Strengthening Restorative Justice in Large-Scale, Anonymous Victim Cases. The findings also indicate that criminal law alone cannot provide complete justice in data breach cases involving millions of victims, many of whom are anonymous or difficult to identify. Accordingly, restorative justice should be operationalized through scalable mechanisms that do not depend on individualized victim identification at the outset. First, mandatory breach notification should function as a restorative baseline, allowing affected individuals to adopt protective measures (account monitoring, credential resets, fraud alerts) and reducing downstream harm. Where victim identification is uncertain, notification can be structured in tiers, beginning with public notification and risk communication, followed by individualized notices when contact data becomes available through forensic verification and controller records (United Nations, 2018).

Second, compensation and restoration can be implemented through administrative claims and standardized redress schemes, including a dedicated compensation fund financed by disgorgement of unlawful gains, administrative fines, or court-ordered payments for aggravated cases. Such a mechanism would allow victims to claim compensation using verifiable harm indicators (e.g., fraudulent transactions, identity misuse reports) without requiring full criminal adjudication in every instance. Third, restorative justice can include mandatory corrective measures imposed on responsible entities security upgrades, third-party audits, and compliance monitoring to prevent recurrence and ensure that restoration includes future risk reduction rather than compensation alone. These restorative components complement criminal sanctions by improving victim recovery, strengthening public trust, and aligning enforcement with the preventive aims of data protection (European Union, 2016; United Nations, 2018).

Preventing Over-Criminalization and Protecting Non-Malicious Businesses. While the establishment of a Specialized Cyber Data Protection Taskforce is a strong practical recommendation, the study’s findings also require safeguards against over-criminalization. Not all personal data incidents involve intent to trade or profit, and an overly punitive regime could discourage transparency, breach reporting, and compliance investment. Therefore, a tiered sanction framework should explicitly differentiate willful data trafficking from negligent or non-malicious security failures. Intent-based categorization willful, reckless, negligent would preserve proportionality and ensure that criminal penalties focus on actors whose conduct reflects culpable exploitation of personal data (Hart, 1968).

In practice, this approach can be operationalized through (1) safe-harbor principles for organizations that promptly report breaches, cooperate with investigations, and demonstrate compliance with security obligations; and (2) reserving criminal liability for cases involving intentional sale, brokerage, or knowing facilitation of unlawful data trading. For unintentional leaks, administrative enforcement and corrective obligations should remain primary, with criminal sanctions triggered only where evidence shows deliberate misconduct, concealment, or repeated non-compliance causing severe harm (Royal Thai Government Gazette, 2019; European Union, 2016). Such safeguards would reduce chilling effects on innovation and compliance while enabling decisive prosecution of data traffickers and organized illicit markets.

Finally, the results underscore that criminal law is necessary but not sufficient. Effective deterrence emerges when criminal provisions operate within a multilayered governance system: risk-based administrative oversight, meaningful civil remedies, auditable security obligations, and sectoral codes of practice for platforms that host or facilitate data transactions. Embedding restorative elements—victim notification, standardized redress mechanisms, mandated security upgrades, and disgorgement of unlawful gains—can further align sanctions with the preventive aims of data protection. Taken together, these measures would close the most salient doctrinal and institutional gaps identified in this study while honoring constitutional principles of fairness, proportionality, and legal certainty.

Suggestions

This research highlights the need for Thailand to strengthen its legal, institutional, and policy frameworks to effectively combat the unlawful sale of personal data and align domestic practices with international standards. Based on the findings, the following recommendations are proposed to enhance criminal law enforcement and improve the effectiveness of penal sanctions in this area.

1. Legislative reform, legality, and a clear definition of unlawful data sale. The Personal Data Protection Act B.E. 2562 (PDPA) should be amended to explicitly criminalize personal data trafficking by private actors and to satisfy the principle of legality (Hart, 1968). A clear statutory

definition should be introduced. For example, *"unlawful data sale"* may be defined as: the intentional buying, selling, exchanging, brokering, advertising, or distributing personal data obtained or used without lawful basis or valid consent, for profit or other benefit, where the actor knows or should reasonably know the illegality of the transaction. This definition should apply to any person, not only officials, and incorporate aggravating factors such as large-scale datasets, vulnerable groups, or sensitive biometric/health data. Consistent with the United Kingdom's Data Protection Act 2018 (DPA 2018) (ss.170–171), criminal liability should extend to individuals and organizations engaging in unauthorized data transactions (legislation.gov.uk, 2024). Penalties should be tiered and proportionate to harm and economic gain, reflecting deterrence-oriented benchmarks under the GDPR and the CCPA (European Union, 2016; State of California Department of Justice, Office of the Attorney General, 2024).

2. Institutional strengthening and enforcement capacity. The Personal Data Protection Committee (PDPC) should be granted independent investigative and prosecutorial powers modeled after the UK's ICO, supported by a specialized Cyber Data Protection Taskforce to address evidentiary and jurisdictional challenges in digital investigations (United Nations, 2018; ICO, 2023).

3. Data-sharing agreements with strict safeguards. Data Sharing Agreements and cross-border cooperation mechanisms should be developed, but only under strict safeguards: purpose limitation, data minimization, access controls, audit trails, retention limits, and accountability for misuse, to ensure that cooperation does not create new privacy risks (European Union, 2016).

4. Mandatory DPIAs for sensitive data. Data Protection Impact Assessments (DPIAs) should be a mandatory prerequisite not merely recommended for any entity processing or transferring sensitive biometric or health records, with periodic audits and enforceable remediation requirements to align prevention with sanction-based deterrence (European Union, 2016).

Reference

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M., Levi, M., Moore, T., & Savage, S. (2019). *Measuring the changing cost of cybercrime*. Proceedings of the 28th International World Wide Web Conference (WWW 2019), 1–11. https://doi.org/10.1145/3308558.3313537

BBC News Thai. (2024, March 17). *PDPA: What can and cannot be done under Thailand's Personal Data Protection Act and the exceptions to consent requirements*. https://www.bbc.com/thai/thailand-61642823

Computer Crime Act B.E. 2550 (2007) (as amended by the Computer Crime Act (No. 2) B.E. 2560 (2017)). *Royal Thai Government Gazette.*

Constitution of the Kingdom of Thailand. (2017). *Constitution of the Kingdom of Thailand B.E. 2560 (2017).* Government of Thailand. https://constitutionnet.org/sites/default/files/2017-05/CONSTITUTION+OF+THE+KINGDOM+OF+THAILAND+(B.E.+2560+(2017)).pdf

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications. https://books.google.co.th/books?id=gX1ZDwAAQBAJ

Criminal Code B.E. 2499 (1956). *Royal Thai Government Gazette.*

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, L 119*, 1–88.

Government of Thailand. (2017). *Constitution of the Kingdom of Thailand B.E. 2560 (2017).* Government of Thailand.

Hart, H. L. A. (1968). *Punishment and responsibility: Essays in the philosophy of law.* Clarendon Press. PhilPapers

Information Commissioner's Office (ICO). (2023). *Data Protection Act 2018.* https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-protection-act-2018/ ICO

Khamsom, J., Areerat, T., & Lekdee, A. (2024). Development of an information management model in accordance with the Personal Data Protection Act for Rajabhat Universities.

Journal of Technology Management Rajabhat Maha Sarakham University, 11(1), 42–55. https://ph02.tci-thaijo.org/index.php/itm-journal/article/view/253003 Thai Journal Online

Legislation.gov.uk. (2024). *Data Protection Act 2018.* Retrieved March 18, 2025, from https://www.legislation.gov.uk/ukpga/2018/12/contents Legislation.gov.uk

Miles, M. B., Huberman, A. M., & Saldaña, J. (2019). *Qualitative data analysis: A methods sourcebook* (4th ed.). SAGE Publications. https://www.metodos.work/wp-content/uploads/2024/01/Qualitative-Data-Analysis.pdf

Office of the Personal Data Protection Committee. (2024a, March 17). *PDPA information guide.* https://www.pdpc.or.th/pdpc-book/pdpa-information

Office of the Personal Data Protection Committee. (2024c, March 18). *European Union Convention on the Protection of Personal Data.* https://www.pdpc.or.th/3442/

Personal Data Protection Act B.E. 2562 (2019). *Royal Thai Government Gazette.*

Rattanapornsuwan, N. (2023). Public awareness and understanding of the Personal Data Protection Act among citizens in Bangkok. *Journal of Roi Kaensarn Academi, 8*(9), 200–208. https://so02.tci-thaijo.org/index.php/JRKSA/article/view/262948

Royal Thai Government Gazette. (2019, May 27). *Personal Data Protection Act B.E. 2562 (2019)* (*Vol.* 136, *Part* 69 A). https://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF

State of California Department of Justice, Office of the Attorney General. (2024, March 18). *California Consumer Privacy Act (CCPA).* https://oag.ca.gov/privacy/ccpa

Suraratchai, R. (2023). The guidelines for personal data protection in criminal investigation. *Chulalongkorn Law Journal, 41*(1), 103–137. https://so01.tci-thaijo.org/index.php/lawchulajournal/article/view/263374/173184

United Nations Human Rights Council. (2018). *Promoting and protecting human rights in the context of the illicit trade in personal data* (A/HRC/39/49). United Nations. https://docs.un.org/en/A/HRC/39/49

United Nations Human Rights Council. (2018). *Promoting and protecting human rights in the context of the illicit trade in personal data* (A/HRC/39/49). United Nations. https://docs.un.org/en/A/HRC/39/49

Wipulakhom, S., & Pitiyasak, S. (2021). Problems concerning personal data protection laws: A case study of biodata types. *Veridian E-Journal, Silpakorn University, 34*(2), 36–59. https://he02.tci-thaijo.org/index.php/Veridian-E-Journal/article/view/153571/111846

Wolford, B. (2024). *What is GDPR, the EU's new data protection law?* GDPR.EU. https://gdpr.eu/what-is-gdpr/ GDPR.eu