International Journal of Multidisciplinary Research and Development
www.allsubjectjournal.com
ISSN Online: 2349-4182 ISSN Print: 2349-5979
Received: 23-05-2025, Accepted: 22-06-2025, Published: 08-07-2025
Volume 12, Issue 7, 2025, Page No. 39-42

The public prosecutor's discretion in ordering criminal case about digital evidence in Thailand

Sonthon Khongwan
Faculty of Science, Graduate School of Forensic Science and Criminal Justice, Silpakorn University, Thailand

Abstract
Advancements in science and information technology have significantly impacted the rise of computer-related crimes in Thailand, posing critical challenges to the collection and evaluation of digital evidence. Within the Thai criminal justice system, public prosecutors play a pivotal role in exercising discretion on whether to prosecute or dismiss a case. This discretion becomes increasingly complex in criminal cases involving digital evidence, where prosecutors face challenges in assessing the credibility and reliability of such evidence.

This study aims to examine the issues surrounding prosecutorial discretion in handling criminal cases involving digital evidence. Utilizing a qualitative research methodology and in-depth interviews, the findings reveal that while prosecutors recognize the importance of digital evidence in cybercrime cases, problems persist in several key areas. These include the legal enforcement framework, standards of forensic examination, evidence collection procedures, and prosecutors' understanding of digital evidence. These factors contribute to inconsistencies in the exercise of prosecutorial discretion regarding the acceptance or rejection of digital evidence. Based on these findings, this study proposes several solutions: legal reform, the development of standardized protocols for digital evidence collection aligned with international standards, and targeted training programs for prosecutors. These measures aim to enhance prosecutors' knowledge and provide them with the necessary tools to evaluate the reliability of digital evidence effectively.

Keywords: Prosecutorial discretion, public prosecutor, digital evidence, criminal case

Introduction

The advancement of science and information technology has created unprecedented opportunities for criminals to commit offenses and exploit technology for malicious purposes. The emergence and application of new technologies have enabled novel forms of crime that were previously inconceivable—crimes in which technology serves not only as a medium of communication but also as a tool to target victims or facilitate illegal activities that may not be possible in the physical world (Holt and Bossler, 2016) [7]. Analysis of cybercrime trends indicates a significant rise in both the volume and variety of offenses, primarily driven by the rapid proliferation of mobile devices and internet access (Butkovic *et al*.,2019) [2].These developments have made it easier for offenders to reach their victims. Although the motivations of cybercriminals may be similar to those of traditional criminals, the former often employ far more sophisticated technological means, thereby presenting greater challenges for law enforcement (Sarkar and Shukla, 2023) [11]. In cybercrime cases, digital evidence is defined as any information that can demonstrate the commission of a crime or establish a link between the crime, the victim, and the perpetrator (Casey, 2011) [3]. The increasing reliance on digital evidence has introduced new complexities and challenges to the Thai criminal justice system, particularly regarding prosecutorial discretion in deciding whether or not to prosecute a case in court. The acceptance or rejection of digital evidence by prosecutors now involves more intricate considerations concerning the integrity, credibility, and probative value of such evidence—issues that demand careful assessment and a sound understanding of technological aspects and their implications for justice.

The concept of prosecutorial discretion lies at the heart of the criminal justice system, especially in Thailand, where the principle of public prosecution is upheld. Prosecutors are responsible for handling cases during the pretrial stage and are guided by the opportunity principle (Na Nakhon, 2018) [9], which allows them to determine whether or not to pursue a criminal prosecution. This discretionary power plays a vital role in the efficiency and fairness of the justice system, enabling prosecutors to weigh various factors in managing cases (Thongjean and Sirivunnabood, 2015) [15]**.** However, the exercise of such discretion is inherently complex and often subject to scrutiny and debate, particularly regarding its potential implications for justice (Bellin, 2020) [1] Given that prosecutors act as a bridge between law enforcement and the judiciary, their role is of strategic importance; all criminal cases must pass through prosecutorial review before entering judicial proceedings.

This study primarily aims to examine the legal issues and contributing factors that influence the exercise of prosecutorial discretion in managing criminal cases involving digital evidence in Thailand. The objective is to enhance transparency in prosecutorial decision-making and ensure its alignment with forensic principles. The study also seeks to establish a practical framework that balances the challenges of managing digital evidence with the need to safeguard the rights of both defendants and victims through the appropriate use of discretion. In addition, this research includes an in-depth analysis of legal issues and practices related to digital evidence, with the ultimate goal of developing actionable recommendations to strengthen the effectiveness of prosecutorial discretion in this evolving context.

Research Methods

This study aims to examine the problems and obstacles associated with the exercise of prosecutorial discretion in accepting or rejecting digital evidence within the Thai criminal justice system. A qualitative research methodology

was employed, consisting of two key components:

1. Documentary Research

A systematic literature review was conducted using academic sources from reputable national and international databases, including Scopus, SSRN, and TCI (Thai Journal Citation Index), covering the period from 2015 to 2024. The purpose of this stage was to identify and evaluate the core body of knowledge related to prosecutorial discretion, digital evidence examination, and legal enforcement frameworks.

2. In-depth Interviews

The researcher conducted in-depth interviews with ten public prosecutors who have direct experience dealing with digital evidence. Participants were selected through purposive sampling. This phase aimed to uncover practical challenges and obstacles faced by prosecutors in deciding whether to admit or reject digital evidence, as well as to gather their recommendations for addressing such challenges.

Data Analysis Process

Data collected from the first phase served as the primary source for analyzing the issues and constraints in the exercise of prosecutorial discretion concerning digital evidence. The data from the second phase was used to support and enrich the findings from the first phase. The results from both phases were systematically analyzed and synthesized using descriptive analytics. A content analysis technique was applied to identify themes, causes, and implications, culminating in conclusions that provide insight into the problems and offer practical recommendations for enhancing the reliability of prosecutorial decisions related to digital evidence in Thailand's criminal justice system.

Results and Discussion

The findings of this study reveal that the exercise of prosecutorial discretion in accepting digital evidence is influenced by several interrelated factors, as follows:

1. Legal Framework Governing Prosecutorial Discretion

In Thailand, the legal framework serves as a fundamental guideline for prosecutors in the exercise of their discretion and is considered a cornerstone of the criminal justice process. This framework outlines the scope and principles that guide prosecutors in deciding whether to prosecute, dismiss, or amend charges, particularly in relation to digital evidence submitted by investigating officers. Thus, an effective and clear legal framework is essential to support prosecutors in making sound discretionary decisions.

The research indicates that several legal instruments define the prosecutorial discretion in Thailand, including: The Criminal Procedure Code (Sections 140, 141, 143, 145/1), The Public Prosecutor Organization and Public Prosecutors Act B.E. 2553 (2010) (Sections 21, 22), The Regulation of the Office of the Attorney General on Criminal Prosecution B.E. 2563 (2020) (Sections 8, 22). All these statutes emphasize the principles of independence and fairness in prosecutorial decision-making. In cases of non-prosecution, the law allows prosecutors to exercise discretion when the act does not constitute a crime, the evidence is insufficient, or the case does not serve the public interest. However, the study found that while these legal provisions outline case management procedures, they do not clearly define how discretion should be exercised specifically in the context of digital evidence. This lack of clarity hinders prosecutors' ability to evaluate the validity and suitability of digital evidence for use in court. These findings are consistent with those of Netipatalachoochote (2009) [10], who concluded that prosecutorial discretion in Thailand lacks adequate standardization, particularly in the context of criminal cases.

2. Type of Digital Evidence

Digital evidence is typically presented in electronic data formats, which differ from physical evidence such as weapons or loan documents. Digital evidence is stored and represented in binary format (0 and 1), which are used to convey characters, numbers, and symbols recognizable to humans. This inherent nature makes digital evidence fundamentally different from traditional physical or documentary evidence.

The research findings show that there is ongoing debate about how digital evidence should be classified under current legal frameworks. The legal definitions of documentary and physical evidence do not adequately cover the unique nature of digital data. This creates challenges for how digital evidence is presented in court and affects prosecutors' ability to determine the appropriate form for its submission. These findings align with the works of Srisuwan (2021) [12] and Jaisue (2021) [8], both of whom argue that electronic data should be categorized as a distinct type of legal evidence due to its special characteristics.

3. Standards for Collecting Digital Evidence

The standards governing evidence collection are crucial in determining the admissibility and credibility of digital evidence. In the context of prosecutorial discretion, prosecutors must assess whether digital evidence has been collected in accordance with legal requirements and international best practices. Any deviation from these procedures can compromise the integrity of the evidence.

The study found that prosecutors are aware of the necessity for digital evidence to be collected under standardized procedures. This ensures they can properly evaluate its reliability. Any procedural flaws in evidence collection can affect the completeness of the evidence and may ultimately lead to the rejection of such evidence in court. These findings are consistent with the research of Stoykova *et al*. (2022), which emphasizes that the credibility of digital evidence depends on internationally accepted standards and best practices widely recognized within the digital forensics' community.

4. Digital Evidence Examination Process

Digital evidence is the result of scientific methodologies and tools that ensure "its authenticity and integrity can be validated" (Stoykova, 2021) [13]. Therefore, the process of examining digital evidence serves as a fundamental basis for establishing the credibility and admissibility of such evidence in criminal investigations. Prosecutors must evaluate whether the digital evidence examination process strictly adheres to relevant technical and legal standards. The prosecutor's discretion is vital in determining whether the forensic process used to handle digital evidence is reliable and lawfully conducted.

The study found that the examination of digital evidence in Thailand remains a relatively new practice. However, its

significance is growing rapidly within the criminal justice process. While prosecutors generally emphasize the legality of evidence acquisition—such as whether search, seizure, and arrest procedures comply with legal requirements—they often overlook the technical integrity of the digital evidence examination process itself. For example, during evidence collection, it is crucial to ensure that the data has not been altered or contaminated. In the analysis phase, the use of validated tools and scientifically accepted methodologies is essential to generate accurate results that comply with forensic standards. Failure to evaluate these technical aspects may compromise the integrity of the evidence and ultimately affect its admissibility in court.

5. Standards of Digital Forensics Agencies

The standards governing digital forensic agencies play a vital role in ensuring the credibility and admissibility of digital evidence in criminal cases. These standards encompass technical protocols, the certification of tools and personnel, and adherence to internationally recognized best practices. Their purpose is to ensure that digital evidence is handled properly, thereby reducing the risk of tampering, data loss, or procedural errors.

The study found that in Thailand, prosecutors tend to overlook the issue of agency standards when evaluating digital evidence. This is largely due to the perception that such matters fall under the jurisdiction of external agencies. Prosecutors generally assume that digital forensic agencies, such as the Central Police Forensic Science Division and the Central Institute of Forensic Science Thailand, already operate under reliable standards, as they are government institutions. As a result, prosecutors rarely question or verify whether digital evidence has been processed in compliance with agency-level quality standards.

6. Chain of Custody for Digital Evidence

The chain of custody is a critical factor influencing the admissibility and credibility of digital evidence in criminal proceedings. Prosecutors must carefully verify the integrity of the chain of custody to ensure the preservation of the original data and the reliability of the methods and tools used in its handling. Any breach or irregularity in the chain of custody may significantly impact the prosecutor's discretion in determining the evidentiary value of digital evidence.

The study reveals that prosecutors recognize the importance of maintaining a robust and verifiable chain of custody for digital evidence. However, challenges persist due to the inherent complexity of digital data. Digital evidence is more susceptible to alteration, duplication, or unauthorized modification compared to physical evidence. These vulnerabilities make it more difficult for prosecutors to verify the continuity and accuracy of the chain of custody. As a result, there is a risk that prosecutorial discretion may be exercised with uncertainty or caution when the integrity of the evidence cannot be confidently assured. These findings are consistent with the research of D'Anna *et al*. (2023) [4], who noted that: **"**The chain of custody is the most important and, at the same time, the most critical process of documenting evidence**"**.

This underscores the need for rigorous procedures, standardized documentation, and technological literacy among prosecutors to effectively evaluate the chain of custody in digital forensic contexts.

7. Prosecutors' Knowledge and Understanding

The knowledge and expertise of prosecutors play a crucial role in the effective exercise of discretion in criminal cases involving digital evidence. A comprehensive understanding of the limitations, conditions, and characteristics of various types of forensic evidence, as well as the implications of scientific examination results, is essential for integrating forensic findings with applicable legal principles (Faculty of Applied Science, 2016) [6]. Insufficient knowledge may hinder prosecutors' ability to assess the reliability, admissibility, and relevance of digital evidence—thereby affecting the soundness of their discretionary decisions.

The findings of this study indicate that awareness and understanding of digital evidence among Thai prosecutors remain limited, as digital forensics is still a relatively new field within the justice system. This lack of knowledge directly affects prosecutors' capacity to evaluate digital evidence submitted by law enforcement agencies and diminishes their ability to effectively question forensic experts during courtroom proceedings. These findings align with the study by Erlandsen (2019) [5], which warns that: "Without a clearer understanding of the complexity of digital evidence, prosecutors risk making errors that may lead to miscarriages of justice."

The results highlight the urgent need for capacity building and targeted training in digital evidence for prosecutors to enhance their evaluative capabilities and uphold the integrity of the criminal justice process.

Conclusion

The growing reliance on digital evidence has transformed the landscape of Thailand's criminal justice system, introducing new layers of complexity. This shift directly impacts both law enforcement agencies and justice sector personnel, who must enhance their competencies to ensure that criminal proceedings are conducted fairly and effectively.

The findings of this research reveal a range of challenges affecting prosecutorial discretion in cases involving digital evidence. Therefore, it is essential for prosecutors to adopt clear and effective frameworks to guide the exercise of discretion in such cases.

This study proposes the following recommendations

- **Short-term:** Prosecutors should receive targeted training to build their understanding of digital forensic processes, including legal and technical aspects.
- **Long-term:** A dedicated digital forensics unit within the Office of the Attorney General of Thailand should be established to support prosecutors in handling cases involving digital evidence.
- Additionally, legal reforms are urgently needed—particularly regarding the investigative powers of prosecutors and their role in overseeing digital evidence in criminal cases.

These steps will help ensure that prosecutorial discretion is exercised with both fairness and competence in an era increasingly shaped by digital evidence.

References

1. Bellin J, Theories of Prosecution. California Law Review,2020:108:1203-1253,

https://www.californialawreview.org/print/theories-of-prosecution.
2. Butkovic A, Mrdovic S, Uludag S, Tanovic A. Geographic profiling for serial cybercrime investigation. Digital Investigation,2019:28:176-182.
3. Casey, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd) : Elsevier Inc, 2011.
4. D'Anna T, Puntarello M, Cannella G, Scalzo G, Buscemi R, Zerbo S. *et al* The Chain of Custody in the Era of Modern Forensics: From the Classic Procedures for Gathering Evidence to the New Challenges Related to Digital Data. Healthcare (Basel, Switzerland),2023:11(5):634. https://doi.org/10.3390/healthcare11050634.
5. Erlandsen TE, Fallacies when Evaluating Digital Evidence Among Prosecutors in the Norwegian Police Service, (Master's thesis, Norwegian University of Science and Technology), 2019. http://hdl.handle.net/11250/2617771.
6. Faculty of Applied Science, The Development of Forensic Evidence Adhesion Guidelines to Prove the Truth of the Case (Research Report), https://rabi.coj.go.th/th/content/category/detail/id/39/iid/176580, 2016.
7. Holt JT, Bossler MA. Cybercrime in Progress Theory and prevention of technology-enabled offenses. New York: Routledge, 2016.
8. Jaisue N, Legal Measure of Admissibility of Digital Evidence. Rajabhat Maha Sarakham University Journal,2021:15(1):109–121.
9. Na Nakhon K, criminal procedure law, 9th ed. Bangkok: Winyuchon, 2018.
10. Netipatalachoochote S, Prosecutor's Standards in Exercising Discretion to Prosecute, (Master's thesis, Thammasat University) https://digital.library.tu.ac.th/tu_dc/frontend/Info/item/dc:124715, 2009.
11. Sarkar G, Shukla SK. Behavioral analysis of cybercrime: Paving the way for effective policing strategies. Journal of Economic Criminology, 2023, 2, 100034.
12. Srisuwan K, Digital Forensics Evidence Proving Process: An Analytic Approach to Policy Development, (Doctoral dissertation, Chulalongkorn University) https://digital.car.chula.ac.th/chulaetd/5662, 2021.
13. Stoykova R, Digital evidence: Unaddressed threats to fairness and the presumption of innocence, Computer Law & Security Review, 2021, 42, 105575, https://doi.org/10.1016/j.clsr.2021.105575.
14. Stoykova R, Andersen S, Franke K, Stefan Axelsson S, Reliability assessment of digital forensic investigations in the Norwegian police, Forensic Science International: Digital Investigation, 40, 301351, https://doi.org/10.1016/j.fsidi.2022.301351, 2022.
15. Thongjean A, Sirivunnabood P. The Principles of Public Prosecutor's Discretion Not Prosecuting the Non Public Interest Criminal Cases in Thailand. Thammasat Review,2015:16(2):1–19. https://sc01.tci-thaijo.org/index.php/tureview/article/view/40750.