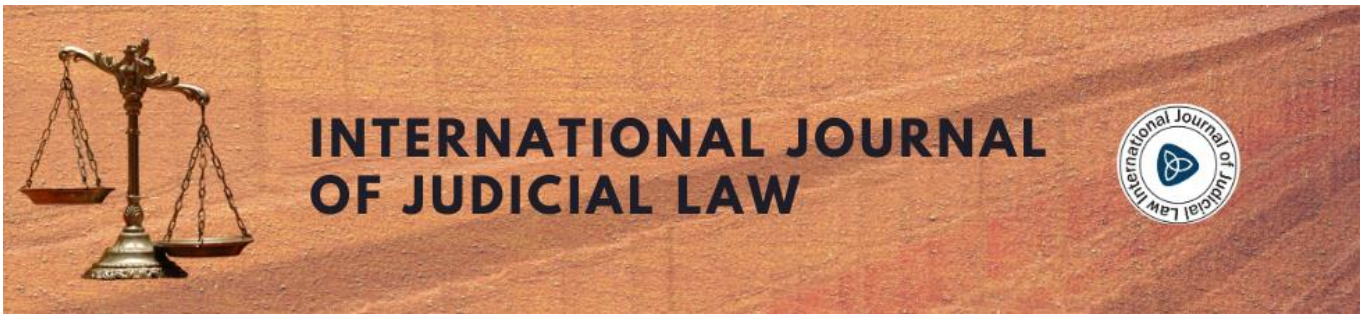




The Role of Digital Forensics in Proving Criminal Cases of Personal Data Misuse

Rudiansyah ^{1*}, Ahmad Syaafi ²

¹ Master of Law Program Student, Faculty of Law, Lambung Mangkurat University, Indonesia

² Lecturer at Faculty of Law, Lambung Mangkurat University, Banjarmasin, Indonesia

* Corresponding Author: Nurjanah

Article Info

ISSN (online): 2583-6536

Volume: 04

Issue: 03

May-June 2025

Received: 13-04-2025

Accepted: 15-05-2025

Page No: 122-127

Abstract

In today's digital era, the development of information technology has had a significant impact on various aspects of human life, including in the legal field. One of the main challenges that arises is the protection of personal data. Personal data is information that is private and confidential, which if misused can cause great harm, both to individuals and society at large. Law Number 27 of 2022 concerning Personal Data Protection which has been enacted in Indonesia aims to ensure the security and confidentiality of such data, as well as provide legal guarantees for data owners. Cybercrimes involving violations of personal data protection are often difficult to uncover due to the complexity of the technology used by the perpetrators. Therefore, a more sophisticated and integrated approach is needed to resolve these cases. Digital forensic technology is one of the important tools in resolving criminal cases of personal data misuse. However, the use of digital forensic technology in handling cases of personal data misuse still faces various obstacles.

The type of research used is normative legal research using a legislative approach and a conceptual approach.

The results of the study show that digital forensics has a strategic role in proving criminal cases of personal data abuse, especially in presenting legal, valid, and legally accountable electronic evidence. Through systematic forensic techniques, the perpetrator's digital footprint can be identified, analyzed, and presented as evidence that supports the law enforcement process.

DOI: <https://doi.org/10.54660/IJL.2025.4.3.122-127>

Keywords: Digital Forensics, Evidence, Criminal Acts, Personal Data

1. Introduction

The development of information technology is now very fast and very different from the early days of its presence. The era of globalization has placed the role of information technology in a very strategic position because it can present a world without limits, distance, space, and time and can increase productivity and efficiency. Information technology has changed the lifestyle of society globally and caused changes in socio-cultural, economic, and legal frameworks that took place quickly and significantly. Technological advances have resulted in a number of situations that were never thought of before by humans ^[1]. The problem of personal data security has become a very important global issue in the current era, due to the progress of development towards the era of the Web of the World which is marked by the progress of communication between humans using mobile communications such as smartphones and computers connected to the internet, ^[2] where the internet connects the physical world into a network called cyberspace ^[3].

¹ Diaz Gwijangge. (2011), "Peran TIK Dalam Pembangunan Karakter Bangsa," (makalah disampaikan dalam Workshop: "Pemanfaatan Jejaring E-Pendidikan" yang diselenggarakan Pusat Teknologi Informasi dan Komunikasi Pendidikan Kementerian Pendidikan Nasional, Sulawesi Selatan, 14 Juni 2011.

² Sinta Dewi Rosadi. (2015), *Cyber Law: Aspek Data Pribadi Menurut Hukum Internasional, Regional, dan Nasional*, Bandung: Refika Aditama, p. 1.

³ Tutorials Point, "information security & cyber law", www.tutorialspoint.com, accessed on January 26, 2025.

However, the increasing use of technology is also accompanied by various threats to personal data security, such as data theft, hacking, and misuse of information.

Cybercrimes involving violations of personal data protection are often difficult to uncover due to the complexity of the technology used by the perpetrators. Therefore, a more sophisticated and integrated approach is needed to solve these cases.

Digital forensic technology is one of the important tools in solving criminal cases of personal data abuse. This technology includes various methods and techniques to identify, analyze, and recover digital evidence relevant to a case. By utilizing digital forensic technology, law enforcement officers can track digital traces left by perpetrators, understand attack patterns, and collect evidence that can be used in court.

However, the use of digital forensic technology in handling cases of personal data abuse still faces various obstacles. One of them is the limited human resources who have expertise in this field. In addition, the rapid development of technology often makes regulations and legal policies lag behind, thus causing uncertainty in the law enforcement process.

Based on this background, research on the role of digital forensics in proving criminal cases of personal data misuse is very important to conduct.

2. Research Results and discussion

The rapid development of information and communication technology has provided many benefits in human life, especially in terms of efficiency and accessibility of information. However, behind this progress, there are also serious challenges in the form of cybercrime, one of which is the misuse of personal data. Misuse of personal data is an illegal act that can include theft, collection, processing, distribution, or sale of individual information without the owner's consent. This crime is becoming increasingly rampant along with the increasing digitalization in various sectors such as banking, e-commerce, education, and government.

Indonesia as a country with a high number of internet users, faces significant risks related to privacy violations and misuse of personal data. Based on the report of the Indonesian Internet Service Providers Association (APJII), in 2023 there will be more than 215 million internet users in Indonesia ^[4]. On the other hand, cases of leaks and misuse of personal data are increasingly occurring, one of which is the incident of a data leak of 1.3 billion prepaid SIM card registration numbers which allegedly came from a database belonging to the Ministry of Communication and Information ^[5].

In 2022–2023, Indonesia was rocked by several major data leak incidents, such as the Bharada E-Mail Kemkominfo, MyPertamina, and BPJS Kesehatan cases, which involved millions of citizens' personal data ^[6]. Investigations into some of these cases have encountered serious obstacles due to the lack of digital forensic expertise in law enforcement agencies and the absence of standard protocols for handling digital evidence.

In some cases, the leaked data is traded on the dark web, and is difficult to trace due to the lack of adequate digital footprints. This confirms that without reliable and responsive digital forensics, perpetrators will continue to escape the law. This phenomenon shows the existence of security gaps and weak supervision and law enforcement regarding personal data protection. Law Number 27 of 2022 concerning Personal Data Protection is an important milestone in the Indonesian government's efforts to protect citizens' privacy rights. However, the effectiveness of the implementation of this law is highly dependent on various factors, including the ability of law enforcement officers to accurately identify, collect, and analyze digital evidence. This is where the role of digital forensics becomes very important.

The crime of misuse of personal data has special characteristics, namely digital, cross-border, and often carried out anonymously. Conventional evidence is inadequate to prove this crime, because the perpetrator is not physically present and traces of the crime are hidden in the digital system. Therefore, law enforcement in this context requires an approach based on digital evidence or electronic evidence.

Digital evidence tends to be fragile, easily manipulated, and requires special methods for collection and analysis. In addition, many perpetrators use sophisticated techniques such as encryption, VPNs, or spoofing to disguise their identities and locations. In these situations, only digital forensics can penetrate the complexity.

Digital forensics is a branch of forensic science that focuses on the identification, acquisition, preservation, analysis, and presentation of digital evidence in a legitimate and legally acceptable manner. In the context of personal data abuse, digital forensics is an important tool for tracing the digital footprint of the perpetrator, understanding the mechanism of data leakage, and proving the existence of illegal acts scientifically and systematically.

According to the Big Indonesian Dictionary, urgency is "a very important thing; a pressing necessity" ^[7]. This means a situation that requires immediate attention because it concerns vital or crucial interests. In practice, urgency is often used to justify quick action or high priority in decision making.

Winarno Surakhmad, an expert in education and philosophy of science, explains that urgency is closely related to the strategic and situational value of a phenomenon. He states: "Something is said to be urgent if a delay in handling it can cause great losses or hinder the achievement of primary goals." In other words, urgency is not only seen from the current needs, but also from the future consequences that will arise if not addressed immediately.

William N. Dunn, in his book *Public Policy Analysis*, does not mention the term "urgency" directly, but presents a policy evaluation framework based on urgency, feasibility, and effectiveness. Dunn emphasizes that the urgency of a policy problem can be measured by (a) the level of its impact on society; (b) how large the population is affected; and (b) how

⁴ Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2023), *Laporan Survei Penetrasi & Perilaku Pengguna Internet Indonesia 2023*, <https://apjii.or.id/survei2023>, accessed on May 9, 2025.

⁵ CNN Indonesia. (2022), "Diduga Data 1,3 Miliar Registrasi Kartu SIM Bocor, Kominfo Bungkam." <https://www.cnnindonesia.com/>, accessed on May 9, 2025.

⁶ Tirto.id. (2023), *Bocor Lagi: Data Pengguna MyPertamina Dijual di Forum Hacker*. Diakses dari <https://tirto.id>, accessed on April 26, 2025.

⁷ Kamus Besar Bahasa Indonesia (KBBI), Urgensi, Badan Bahasa Kemendikbud RI.

urgent the time is for resolving the problem ^[8]. Urgency according to Dunn has dimensions of time and social value. Problems that cause mass suffering or social instability are often considered more urgent.

Kartini Kartono relates urgency to social reactions to problems. She states that: "A problem becomes urgent when it causes social unrest, challenges the value system of society, or directly threatens social integration" ^[9]. According to Kartini, urgency is an indicator of social pressure that needs to be responded to through collective action, both from society and the state.

From a legal perspective, Soerjono Soekanto explains that the urgency of a policy or legal regulation can be assessed from the community's need for order. He states that "Law is born from the needs of society. When a situation causes unrest, disorder, or conflict, then immediate law is needed - that is why the urgency of the regulation becomes apparent" ^[10]. Soekanto emphasized that urgency in law arises when a legal vacuum creates uncertainty that endangers public order.

In his work *Future Crimes*, Marc Goodman explains that in an increasingly digitalized world, almost all human activities leave digital traces. Therefore, the ability to collect, analyze, and authenticate digital evidence becomes a critical aspect in ensuring security and justice. Goodman states: "The more digital our lives become, the more digital our crimes become, and thus the more urgent our forensic capabilities must be."

^[11] In other words, digital forensics can no longer be seen as optional, but is a mandatory instrument in handling modern crimes.

In their research for the Oxford Internet Institute, Peter Sommer and Ian Brown argue that the urgency of digital forensics encompasses national strategic aspects because digital attacks can threaten a country's critical infrastructure, including banking systems, electricity grids, and electronic government. They emphasize: "Digital forensics is central to the national cybersecurity framework. A failure in digital forensic readiness can render a country vulnerable, not just to crime, but to sabotage and espionage" ^[12]. Thus, from a public policy perspective, digital forensics becomes a vital element in maintaining state sovereignty and resilience against digital attacks.

Nasrullah in his book *Cyber Security and Digital Forensics*, explains that the urgency of digital forensics stems from changes in crime patterns. If in the past the perpetrators and victims were in the same geographical area, now with the internet, the perpetrators could be across continents. He stated, "Digital forensics is the answer to the challenges of cross-border law enforcement in cyberspace. Without the support of strong digital evidence, cybercriminals are

difficult to prosecute" ^[13]. In this case, digital forensics becomes very urgent because it functions as a tool to determine the identity of the perpetrator, location of activity, and the time the crime occurred in a system that is difficult to reach physically.

Cybersecurity expert from Bandung Institute of Technology, Budi Rahardjo stated that the urgency of digital forensics arises due to the lack of capacity of law enforcement in responding to increasingly complex digital attacks. According to him, "Indonesia faces a big challenge in terms of digital forensic capacity. There is a lot of evidence of crime that ultimately cannot be investigated thoroughly because there is no SOP and adequate digital analysis capabilities" ^[14]. This statement emphasizes that the urgent need for strengthening digital forensic capacity in Indonesia is crucial for the effectiveness of law enforcement in the digital era.

Law lecturer from Hasanuddin University, Irwansyah stated that digital forensics is part of the right to justice in the digital era. When someone is harmed through an electronic system, the state is obliged to provide a valid digital evidence mechanism that can be tested in court. He emphasized: "The urgency of digital forensics is not only about technological tools, but also concerns procedural and substantive justice that must be guaranteed by the state" ^[15]. Thus, the state is obliged to strengthen digital forensics as part of its citizens' legal rights, especially in the context of evidence and legal protection.

In its official document, NIJ (United States) emphasizes that "The digital forensic process is time-sensitive and evidence can be lost easily. Therefore, trained personnel, proper SOPs, and forensic tools are urgently required" ^[16]. Digital forensics is very important in the investigation and prosecution process. They said that the success of handling cases, especially technology-based crimes, is very dependent on the quality and speed of the forensic team in finding and authenticating digital evidence. The urgency of digital forensics in this case lies in the vulnerability of digital evidence that can be deleted, changed, or falsified quickly if not immediately secured procedurally.

A researcher and author in the field of information security, Debra Littlejohn Shinder stated that digital forensics has a high level of urgency because it is the only investigative mechanism capable of handling electronic traces that are easily lost or changed. She stated, "Digital evidence is inherently volatile. If not captured in a timely and forensically sound manner, it may be irretrievably lost — thereby undermining the entire investigation" ^[17]. According to Shinder, the urgency of digital forensics is due to the characteristics of digital evidence which is very vulnerable

⁸ William N. Dunn. (2017), *Public Policy Analysis: An Introduction*, New York: Pearson, p. 92–95.

⁹ Kartini Kartono. (2005), *Masalah Sosial*, Bandung: Mandar Maju, p. 21.

¹⁰ Soerjono Soekanto. (2007), *Sosiologi Suatu Pengantar*, Jakarta: Rajawali Press, p. 85.

¹¹ Marc Goodman. (2015), *Future Crimes: Inside the Digital Underground*, Doubleday, p. 75.

¹² Peter Sommer & Ian Brown. (2011), *Reducing Systemic Cybersecurity Risk*, Oxford Internet Institute.

¹³ Nasrullah. (2021), *Keamanan Siber dan Forensik Digital*, Yogyakarta: Andi, p. 63.

¹⁴ Budi Rahardjo. (2018), "Tantangan Forensik Digital di Indonesia," makalah dalam Seminar Nasional Keamanan Informasi, Bandung.

¹⁵ Irwansyah. (2022), "Perlindungan Hukum Terhadap Bukti Digital," *Jurnal Hukum dan Teknologi*, Vol. 5 No. 1, p. 45.

¹⁶ National Institute of Justice (NIJ). (2020), "Digital Evidence and Forensics," U.S. Department of Justice.

¹⁷ Debra Littlejohn Shinder. (2011), *Scene of the Cybercrime*, 2nd ed., Syngress, p. 105.

and unstable, thus requiring a fast and procedural response.

John Sammons, author of *The Basics of Digital Forensics*, emphasizes that the urgency of digital forensics is increasing as criminals become more sophisticated and adaptable to technology. This makes traditional investigations no longer sufficient. According to him, "As technology evolves, so do the methods of criminals. Forensics must not only keep up, but anticipate. The urgency lies in this race against criminal innovation" ^[18]. The concept of urgency according to Sammons is rooted in the race between criminal innovation and investigative readiness, which requires digital forensics to continue to adapt rapidly.

Cyber law expert from Padjadjaran University, Sinta Dewi Rosadi stated that the urgency of digital forensics in Indonesia is increasing due to the increasing cases of personal data violations and the weak evidentiary system in court. She explained, "We are facing an era where physical evidence is starting to be abandoned. Many cases of data misuse ultimately cannot be proven legally due to the lack of valid and standardized digital forensics mechanisms" ^[19]. This statement emphasizes that without strong and standardized digital forensics, legal protection in cyberspace cannot be implemented effectively.

The urgency of implementing digital forensics in handling cases of personal data abuse is not only technical, but also legal and social. Technically, digital forensics methods allow investigators to extract evidence from digital devices such as computers, servers, mobile devices, and cloud storage. This process is very crucial considering that cybercriminals often use sophisticated techniques such as encryption, spoofing, anonymizing tools, and the dark web to hide their identities and activities ^[20].

Legally, digital evidence obtained through a legitimate forensic process can be used in court as a basis for prosecution or defense. Unprocedural collection of evidence can make the evidence inadmissible, potentially weakening the law enforcement process. Therefore, the existence of competent digital forensic experts and supporting systems is crucial in a fair and credible legal process ^[21].

Socially, misuse of personal data can cause great harm to individuals, whether in the form of financial losses, defamation, or psychological disorders. Public trust in digital systems and state institutions can also decrease drastically if cases like this are not handled seriously. With a transparent and professional digital forensics process, the public can feel safer and believe that perpetrators of digital crimes will receive appropriate accountability.

Unfortunately, the implementation of digital forensics in Indonesia still faces various challenges. First, the limited human resources with high competence in the field of digital

forensics is still an obstacle. Second, sophisticated and adequate digital forensics laboratory facilities are not evenly distributed, so that several regions have difficulty in handling cases involving digital evidence. Third, aspects of regulation and coordination between law enforcement agencies often overlap and are not optimal ^[22].

In addition, education to the public about the importance of protecting personal data and reporting procedures when becoming victims of abuse is also not evenly distributed. Many victims do not understand the importance of reporting digital crimes or are not aware of the legal channels available. In this case, synergy between law enforcement, government agencies, the private sector, and civil society is needed to form a strong and sustainable personal data protection ecosystem. In the global context, developed countries such as the United States, the United Kingdom, and Germany have developed a well-established digital forensics system with the support of institutions such as the FBI (Federal Bureau of Investigation) and the Europol Cybercrime Center (EC3). They implement international standards such as ISO/IEC 27037 for handling digital evidence and continue to improve human resource capacity through training and certification ^[23].

In the digital era, personal data protection is an important pillar of human rights. When personal data is misused, victims not only suffer material losses, but also psychological and reputational disorders. Digital forensics has emerged as a major weapon in upholding justice in such cases. Therefore, strengthening the capacity, regulation, and awareness of digital forensics must be a national priority to ensure that violations of privacy are no longer crimes without perpetrators.

Indonesia also needs to move in the same direction by strengthening regulations, infrastructure, and investment in education and training in digital forensics. Universities and vocational training institutions can play an important role in producing digital forensics experts who are able to handle the complexity of personal data abuse cases. In addition, international cooperation in terms of technology transfer and knowledge exchange is also an important strategy to improve national capabilities.

With the high urgency and complexity of the challenges faced, digital forensics should be a key element in the national strategy to combat personal data abuse. Fast, accurate, and accountable case handling will be the foundation for creating digital trust, which is essential in the era of digital transformation. Personal data protection is not just about safeguarding information, but also about safeguarding the dignity, security, and freedom of individuals

¹⁸ John Sammons. (2015), *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*, Syngress, p. 8.

¹⁹ Sinta Dewi Rosadi. (2021), "Tantangan Perlindungan Data Pribadi dalam Era Digital," *Jurnal Hukum Siber Indonesia*, Vol. 3 No. 2, p. 37.

²⁰ Eoghan Casey, *Op.Cit.*, p. 43.

²¹ M. Noble, M. Pollitt, & L. Presley. (2000), "Recovering and Examining Computer Forensic Evidence", *Forensic Science Communications*, vol. 2(4), p. 56.

²² Puslitbang Polri. (2020), *Analisis Kesiapan Penegak Hukum dalam Menangani kejahatan Siber di Indonesia*, Jakarta: Puslitbang Polri, p. 45.

²³ International Organization for Standardization. (2012), *ISO/IEC 27037:2012 - Guidelines for identification, collection, acquisition, and preservation of digital evidence*. <https://www.iso.org/>, accessed on April 26, 2025.

in the digital era.

The urgency of implementing digital forensics in handling cases of personal data abuse cannot be postponed. In the digital era, violations of privacy are not only an individual threat, but also a threat to legal legitimacy and social stability. Therefore, the integration of technical, legal, and social aspects must be the main focus in policy development and law enforcement in Indonesia. Without a systematic and comprehensive application of digital forensics, personal data protection will remain an illusion.

Since the enactment of Law Number 11 of 2008 concerning Electronic Information and Transactions, the position of digital evidence has become stronger. Article 5 paragraph (1) states that electronic information and documents are valid legal evidence. This was strengthened by the Constitutional Court through Decision Number 20/PUU-XIV/2016 which stated that electronic information can be used as valid evidence if it meets authentication requirements.

The role of digital forensics in evidence law is as follows:

1. Finding Evidence Invisible to the Naked Eye

Many cases of digital crime leave traces in the form of hidden files, caches, activity logs, or traces of device usage that are not easily recognized by the general public. Digital forensics has special methods and software to uncover these traces, such as the use of EnCase, FTK, or open source tools such as Autopsy and Volatility.

2. Ensuring the Authenticity and Integrity of Evidence

One of the important principles in evidence law is that evidence must be authentic and not engineered. In digital forensics, the use of hash functions such as MD5 or SHA-256 is used to ensure that digital data has not been changed since it was first taken. This supports the chain of custody, the process of recording who accesses or stores evidence during the investigation to the trial.

3. Explaining the Technical Context to Judges

Judges and law enforcement officers often do not have enough technical knowledge to understand digital evidence. This is where the role of digital forensics experts becomes very important, to bridge the understanding between technical aspects and their legal consequences.

However, the use of digital forensics in the practice of evidence cannot be separated from the basic principles of criminal procedural law. Criminal procedural law regulates the procedures for obtaining, storing, and submitting evidence in court legally and fairly. Without the integration of procedural law principles, digital forensic results can become invalid evidence or have no strong evidentiary value before a panel of judges.

Digital forensics has a crucial role in the law of evidence, especially in dealing with technology-based criminal cases. However, in order for its function to be optimal, digital forensics must be carried out with the principles of criminal procedure law, namely legality, accountability, due process, and testability.

3. Conclusion

That digital forensics has a strategic role in proving criminal cases of personal data abuse, especially in presenting legal, valid, and legally accountable electronic evidence. Through systematic forensic techniques, the perpetrator's digital footprint can be identified, analyzed, and presented as evidence that supports the law enforcement process. Digital forensics plays an important role in evidentiary law as a means of presenting legal, relevant, and legally accountable electronic evidence in accordance with the principles of criminal procedure law, such as legality, objectivity, and due process of law in handling cases of criminal acts of personal data abuse.

4. Reference

1. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). Laporan Survei Penetrasi & Perilaku Pengguna Internet Indonesia 2023 [Internet]. 2023 [cited 2025 May 9]. Available from: <https://apjii.or.id/survei2023>
2. CNN Indonesia. Diduga Data 1,3 Miliar Registrasi Kartu SIM Bocor, Kominfo Bungkam [Internet]. 2022 [cited 2025 May 9]. Available from: <https://www.cnnindonesia.com/>
3. Dunn WN. Public Policy Analysis: An Introduction. New York: Pearson; 2017.
4. Goodman M. Future Crimes: Inside the Digital Underground. Doubleday; 2015.
5. Gwijangge D. Peran TIK Dalam Pembangunan Karakter Bangsa [paper presentation]. Workshop: Pemanfaatan Jejaring E-Pendidikan; 2011 Jun 14; Sulawesi Selatan, Indonesia.
6. International Organization for Standardization. *ISO/IEC 27037:2012 - Guidelines for identification, collection, acquisition, and preservation of digital evidence* [Internet]. 2012 [cited 2025 Apr 26]. Available from: <https://www.iso.org/>
7. Irwansyah. Perlindungan Hukum Terhadap Bukti Digital. J Huk Teknol. 2022;5(1).
8. Badan Bahasa Kemendikbud RI. Kamus Besar Bahasa Indonesia. Jakarta: Balai Pustaka.
9. Kartono K. Masalah Sosial. Bandung: Mandar Maju; 2005.
10. Nasrullah. Keamanan Siber dan Forensik Digital. Yogyakarta: Andi; 2021.
11. National Institute of Justice (NIJ). Digital Evidence and Forensics. Washington: U.S. Department of Justice; 2020.
12. Noblett M, Pollitt M, Presley L. Recovering and Examining Computer Forensic Evidence. Forensic Sci Commun. 2000;2(4).
13. Puslitbang Polri. Analisis Kesiapan Penegak Hukum dalam Menangani Kejahatan Siber di Indonesia. Jakarta: Puslitbang Polri; 2020.
14. Rahardjo B. Tantangan Forensik Digital di Indonesia [paper presentation]. Seminar Nasional Keamanan Informasi; 2018; Bandung, Indonesia.
15. Rosadi SD. Cyber Law: Aspek Data Pribadi Menurut Hukum Internasional, Regional, dan Nasional. Bandung: Refika Aditama; 2015.
16. Rosadi SD. Tantangan Perlindungan Data Pribadi dalam Era Digital. J Huk Siber Indones. 2021;3(2).
17. Sammons J. The Basics of Digital Forensics: The Primer

- for Getting Started in Digital Forensics. Syngress; 2015.
18. Shinder DL. Scene of the Cybercrime. 2nd ed. Syngress; 2011.
 19. Soekanto S. Sosiologi Suatu Pengantar. Jakarta: Rajawali Press; 2007.
 20. Sommer P, Brown I. Reducing Systemic Cybersecurity Risk. Oxford: Oxford Internet Institute; 2011.
 21. Tirto.id. Bocor Lagi: Data Pengguna MyPertamina Dijual di Forum Hacker [Internet]. 2023 [cited 2025 Apr 26]. Available from: <https://tirto.id>
 22. Tutorials Point. Information Security & Cyber Law [Internet]. [cited 2025 Jan 26]. Available from: <https://www.tutorialspoint.com>