West Science Law and Human Rights
Vol. 4, No. 03, July 2026, pp. 188~198

The Application of the Principle of Due Process of Law in Arrests and Detentions Based on Electronic Evidence in Criminal Cases

Tumian Lian Daya Purba[1], Silvester Magnus Loogman Palit[2]
[1,2] Universitas Cenderawasih

Article Info

Article history:

Received Jul, 2026
Revised Jul, 2026
Accepted Jul, 2026

Keywords:

Due Process of Law
Electronic Evidence
Arrest and Detention
Criminal Procedure
Normative Legal Analysis

ABSTRACT

The advancement of digital technology has significantly transformed the nature of criminal activities and the methods used in law enforcement, particularly through the increasing reliance on electronic evidence. This study aims to analyze the application of the principle of due process of law in arrests and detentions based on electronic evidence within criminal proceedings. Using a normative legal research approach, this study examines statutory regulations, legal doctrines, and relevant scholarly literature to evaluate whether current legal frameworks adequately protect individual rights. The results indicate that although electronic evidence has been formally recognized as valid legal evidence, its use as the basis for arrest and detention presents significant challenges. The absence of clear technical and procedural standards, particularly in determining "sufficient preliminary evidence," may lead to inconsistencies and potential violations of due process. Issues related to authenticity, integrity, chain of custody, and technical validation of electronic evidence further complicate its reliability. Moreover, the complexity of digital evidence creates an imbalance between law enforcement authorities and suspects, limiting the latter's ability to effectively challenge such evidence. This study concludes that the application of due process of law in cases involving electronic evidence remains inadequate due to gaps in the regulatory framework and limited institutional capacity. Therefore, it is necessary to strengthen legal standards, enhance judicial oversight, and develop technical guidelines to ensure that the use of electronic evidence aligns with fundamental principles of justice and human rights. This research contributes to the development of criminal law by providing a normative evaluation of the intersection between technological advancements and procedural safeguards.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Name: Tumian Lian Daya Purba
Institution Address: Universitas Cenderawasih
e-mail: tlpurba@gmail.com

1. INTRODUCTION

The rapid development of information and communication technology has fundamentally transformed the landscape of criminal activities and law enforcement mechanisms. In the digital era, crimes are increasingly committed through electronic systems, leaving behind digital traces such as emails, chat logs, metadata, and other forms of electronic evidence. Consequently, law enforcement authorities have adapted by relying more heavily on such evidence to investigate, arrest, and detain suspects. This transformation has improved the effectiveness and efficiency of criminal justice processes, particularly through the integration of digital forensics to validate electronic evidence and ensure its integrity [1]. However, it also raises critical concerns regarding the protection of individual rights, as legal frameworks must continuously adapt to ensure that investigative practices remain aligned with due process standards [2].

The principle of due process of law remains a cornerstone of modern legal systems, guaranteeing fairness, legality, and fundamental safeguards such as the presumption of innocence, the right to legal counsel, and protection against arbitrary detention. In practice, due process functions as a balancing mechanism between state authority and individual rights, particularly in criminal proceedings. Nevertheless, the growing reliance on electronic evidence introduces significant challenges, including the risk of unlawful surveillance, coercive evidence collection, and inconsistencies in digital forensic standards that may undermine legal certainty [1], [2]. Furthermore, the emergence of advanced technologies such as artificial intelligence complicates this balance, requiring adaptive legal strategies to ensure that law enforcement effectiveness does not come at the expense of civil liberties [3]–[5].

In many jurisdictions, including Indonesia, the legal recognition of electronic evidence has been formally established through statutory regulations, where electronic information and documents are considered valid legal proof as long as they meet the requirements of authenticity, integrity, and reliability. This recognition has significantly transformed the evidentiary landscape; however, it also raises concerns regarding the extent to which electronic evidence alone can justify the deprivation of individual liberty. The abstract and technical nature of digital evidence often makes it difficult for suspects and even legal practitioners to fully understand or challenge its validity, thereby increasing the risk of misuse or overreliance without adequate procedural safeguards. These challenges are further exacerbated by issues in validating electronic evidence, such as the lack of standardized digital forensic procedures and weaknesses in maintaining the chain of custody, which may undermine legal certainty [1], [6]. Additionally, the ambiguity in judicial interpretation of what constitutes "sufficient preliminary evidence" complicates the application of electronic evidence in criminal proceedings [7].

Furthermore, the use of electronic evidence raises serious implications for the principle of due process of law, particularly when it becomes the primary basis for arrest and detention. The risk of misuse is evident in situations where individuals are subjected to coercive measures based on insufficiently verified digital data, highlighting the danger of overreliance on such evidence [8]. This problem is compounded by gaps in the legal framework, especially within the Indonesian Criminal Procedure Code (KUHAP), which has yet to fully accommodate the complexities of electronic evidence and its procedural safeguards [9]. Moreover, determining the fulfillment of "sufficient preliminary evidence" becomes increasingly complex in the context of digital data, where risks such as data manipulation, unauthorized access, and the use of non-standardized forensic tools can compromise reliability. In practice, these issues have led to instances of arrest or detention based primarily on electronic evidence that has not undergone rigorous verification, thereby raising serious concerns about potential violations of due process rights.

This situation underscores the urgent need to critically examine the application of due process of law in the use of electronic evidence within criminal proceedings. A normative legal analysis is particularly relevant in this context, as it enables a systematic evaluation of existing laws, legal principles, and doctrinal interpretations governing arrests and detentions. By analyzing statutory provisions, legal doctrines, and judicial practices, this study seeks to identify gaps, inconsistencies, and potential areas of reform to ensure that the use of electronic evidence remains aligned with fundamental principles of justice.

The objective of this research is to analyze how the principle of due process of law is applied in arrests and detentions based on electronic evidence, while also assessing whether current legal frameworks provide adequate protection against arbitrary or unjust deprivation of liberty. Furthermore, this study aims to contribute to legal discourse by offering recommendations to strengthen procedural safeguards and enhance the reliability and accountability of electronic evidence in criminal law enforcement. Ultimately, the integration of technological advancements into the criminal justice system must not come at the expense of fundamental rights, as maintaining due process is essential to uphold the rule of law, preserve public trust, and prevent potential abuses of power in the digital age.

2. LITERATURE REVIEW

2.1 Concept of Due Process of Law

The principle of due process of law is a fundamental doctrine in modern legal systems, particularly in criminal justice, requiring the state to respect individual rights and ensure that any deprivation of life, liberty, or property is carried out in accordance with established legal procedures. Rooted in historical developments such as the Magna Carta of 1215, which symbolized limitations on state authority [10], and further shaped by modern jurisprudence, including interpretations by courts that influence various legal systems [11], due process encompasses both procedural and substantive dimensions. Procedural due process emphasizes fair and transparent legal procedures, ensuring that arrests and detentions are based on lawful authority and sufficient evidence, with safeguards such as the presumption of innocence, the right to legal counsel, and protection against arbitrary arrest [12], [13]. Meanwhile, substantive due process focuses on the fairness and reasonableness of laws themselves, preventing unjust infringement on fundamental rights and extending protection across various aspects of individual freedoms [14]. Together, these dimensions function as critical mechanisms to limit excessive state power, uphold accountability, and maintain the legitimacy and integrity of the criminal justice system.

2.2 Arrest and Detention in Criminal Procedure

Arrest and detention are coercive measures that directly affect an individual’s liberty, making them highly sensitive within the framework of due process. In criminal procedure, these actions are generally justified when there is sufficient preliminary or prima facie evidence indicating that a person has committed a crime, although the interpretation of “sufficient evidence” varies across jurisdictions, often leading to inconsistencies and potential violations of individual rights. Legal scholars emphasize that arrest should not be used arbitrarily or as a form of punishment, but rather as a necessary step in the investigation process, while detention must be subject to strict limitations, including time constraints, judicial oversight, and periodic review. International legal frameworks such as the International

Covenant on Civil and Political Rights (ICCPR) highlight principles of legality, necessity, and proportionality, yet in some jurisdictions, including Indonesia, subjective detention criteria and unclear boundaries contribute to legal uncertainty [15]. Similarly, instruments like the European Convention on Human Rights and English common law stress the importance of judicial control to prevent arbitrariness and uphold the rule of law [16]. Pretrial procedures serve as essential safeguards to test the legality of arrest and detention, although their effectiveness varies and often requires stronger institutional frameworks, standardized guidelines, and judicial integrity to function optimally [17], [18]. Ultimately, the absence of clear standards and the persistence of formalistic legal approaches can undermine substantive justice, underscoring the need for legal frameworks that ensure clarity, accountability, proportionality, and alignment with human rights principles [18], [19].

2.3 *Electronic Evidence in Criminal Law*

The emergence of electronic evidence has significantly transformed the evidentiary landscape of criminal law, encompassing digital information such as emails, messages, social media content, metadata, mobile data, and surveillance footage that can be used as legal proof [20]. While widely recognized across jurisdictions, electronic evidence presents unique challenges due to its intangible nature, vulnerability to tampering, and the need for specialized expertise to assess its authenticity, integrity, and reliability, including the importance of maintaining a proper chain of custody [21]. Ensuring its validity requires strict digital forensic procedures such as proper acquisition, preservation, analysis, and presentation yet the lack of standardized procedures often leads to inconsistencies in judicial assessments and threatens legal certainty [1], [22]. Furthermore, the transnational character of digital data introduces additional complexities related to jurisdiction and cross-border access, thereby necessitating comprehensive legal frameworks and stronger international cooperation to harmonize legal standards and ensure the admissibility and reliability of electronic evidence across different jurisdictions [20], [23].

2.4 *Due Process and the Use of Electronic Evidence*

The intersection between due process and electronic evidence has become a central issue in contemporary legal discourse, as the growing reliance on digital data in criminal investigations raises concerns about the potential erosion of fundamental safeguards. While electronic evidence enhances the effectiveness of law enforcement, its use must remain aligned with principles of legality and fairness, particularly in the context of arrest and detention. A key concern is the risk of overreliance on electronic data that may be unlawfully obtained, manipulated, or misinterpreted, potentially leading to wrongful actions and creating imbalances between prosecution and defense due to its technical complexity [5], [24]. The authenticity and integrity of such evidence depend heavily on proper collection methods and a clear chain of custody to prevent tampering and ensure admissibility in court [20], [21]. Additionally, jurisdictional challenges and the transnational nature of digital data further complicate its use, necessitating stronger international cooperation and harmonized legal standards [20]. Therefore, scholars emphasize the need for stricter procedural safeguards, including lawful acquisition, standardized forensic practices, enhanced training for legal actors, and robust judicial oversight, to ensure that electronic evidence is applied responsibly and in full compliance with due process principles [1], [21]

2.5 *Research Gap*

Although numerous studies have discussed due process and electronic evidence separately, there is still a lack of comprehensive analysis focusing specifically on the use of electronic evidence as the basis for arrest and detention. Existing literature often emphasizes the admissibility of electronic evidence in court, but less attention is given to its role in the early stages of criminal proceedings, where decisions about arrest and detention are made. This gap highlights the need for further research to explore how due process principles can be effectively applied in the context of electronic evidence. By addressing this issue, the present study contributes to the development of a more balanced and accountable criminal justice system that integrates technological advancements while safeguarding fundamental rights.

3. METHODS

3.1 Research Approach

This study employs a normative legal research approach, also known as doctrinal research, which focuses on examining legal norms, principles, and doctrines governing the application of due process of law in arrests and detentions based on electronic evidence. This approach analyzes laws as articulated in statutes, regulations, and legal literature rather than empirical societal behavior, making it suitable for evaluating the adequacy and consistency of existing legal frameworks. Through this method, the study aims to assess whether the use of electronic evidence as a basis for arrest and detention aligns with the principle of due process of law and ensures the protection of fundamental rights.

3.2 Type of Research

This research is classified as descriptive-analytical legal research. It is descriptive because it systematically describes the legal rules and principles related to due process, arrest and detention procedures, and the admissibility of electronic evidence. It is analytical because it critically evaluates these legal provisions to identify inconsistencies, ambiguities, and potential gaps in their implementation. The analytical aspect is particularly important in examining how the concept of "sufficient preliminary evidence" is interpreted when electronic evidence is used, and whether such interpretations meet the standards required by due process of law.

3.3 Legal Materials

The study utilizes three categories of legal materials essential in normative legal research, namely primary, secondary, and tertiary legal materials. Primary legal materials consist of binding sources such as statutory regulations governing criminal procedure, arrest and detention, laws regulating electronic evidence, relevant constitutional provisions on human rights and due process, and judicial decisions related to electronic evidence in criminal cases. Secondary legal materials include legal textbooks, scholarly articles, research journals, academic publications, expert opinions, and legal commentaries that support the interpretation and analysis of primary sources. Meanwhile, tertiary legal materials comprise legal dictionaries, encyclopedias, and other reference sources that provide clarification of legal terms and concepts relevant to the study.

3.4 Data Collection Techniques

The data collection method used in this research is library research. This involves systematically collecting legal materials from various sources such as legislation, official documents, academic journals, books, and online legal databases. Library research is appropriate for normative legal studies because it enables the researcher to comprehensively examine legal norms and doctrines without relying on field data. The collected materials are then organized and categorized according to the research objectives.

3.5 Data Analysis Technique

The analysis of legal materials in this study is conducted using a qualitative juridical analysis method, which involves interpreting and examining legal norms, principles, and doctrines to produce logical and systematic conclusions. The analysis is carried out through several stages, including the identification of legal issues related to the use of electronic evidence in arrest and detention, interpretation of legal norms such as statutory provisions and due process principles, and systematization of legal materials by organizing relevant laws and theories into a coherent framework. Furthermore, evaluation and argumentation are applied to assess whether current legal practices align with the principle of due process of law, enabling a critical examination of the relationship between electronic evidence and procedural safeguards in criminal law.

To strengthen the analysis, this research applies several legal approaches, namely the statutory approach, conceptual approach, and case approach. The statutory approach focuses on examining laws and regulations related to criminal procedure and electronic evidence to understand their normative substance. The conceptual approach analyzes key legal concepts such as due process of law, sufficient evidence, and legal certainty based on doctrines and scholarly perspectives. Meanwhile, the case approach involves reviewing relevant court decisions to understand how these legal principles are applied in practice, particularly in cases involving the use of electronic evidence.

4. RESULTS AND DISCUSSION

4.1 Legal Recognition of Electronic Evidence in Criminal Proceedings

The development of digital technology has prompted legal systems to formally recognize electronic evidence as a valid means of proof in criminal proceedings, including in Indonesia, where electronic information and documents are accepted as legal evidence provided they meet requirements of authenticity, integrity, and reliability. This recognition reflects the necessity of adapting legal frameworks to contemporary forms of crime, particularly cybercrime and technology-assisted offenses. In Indonesia, the legal basis for such recognition is established through the Electronic Information and Transactions (ITE) Law, which explicitly acknowledges electronic documents as admissible evidence in court, including their printouts, as long as they comply with applicable legal standards [6], [25], [26].

However, despite this formal recognition, significant challenges remain in the implementation of electronic evidence, particularly in terms of technical verification and judicial interpretation. The absence of detailed procedural guidelines often leads to inconsistencies in how electronic evidence is assessed, highlighting the urgent need for integrating digital forensic practices into the legal system [7]. Digital forensics plays a crucial role in ensuring the authenticity and integrity of electronic evidence, with expert testimony frequently required to validate its reliability in court [6], [8]. At the same time, the reliance on technological processes makes electronic evidence more vulnerable to manipulation, unauthorized access, and misinterpretation compared to conventional forms of proof.

From a normative perspective, the inclusion of electronic evidence significantly expands the evidentiary tools available to law enforcement, enabling investigators to utilize digital traces such as emails, chat logs, transaction records, and metadata to establish criminal elements. Nevertheless, the findings indicate that although the legal system has formally accepted electronic evidence, there remains a lack of comprehensive procedural standards governing its collection, verification, and use especially at early stages such as arrest and detention. This gap creates potential risks in ensuring that electronic evidence is applied consistently with the principle of due process of law, thereby underscoring the need for clearer regulations and stronger procedural safeguards.

4.2 The Concept of Sufficient Preliminary Evidence Based on Electronic Data

A crucial requirement for arrest and detention in criminal law is the existence of "sufficient preliminary evidence," which has traditionally been interpreted based on tangible and testimonial forms of proof. However, the increasing reliance on electronic evidence challenges this conventional understanding, as digital data introduces complexities that require rigorous validation processes to ensure authenticity and reliability. Digital evidence has become essential in modern criminal proceedings, particularly in cases involving cybercrime and fraud, and courts are increasingly willing to accept such evidence provided it complies with established legal and forensic standards [21], [27]. In addition, regulatory developments, such as those introduced in the European Union, aim to facilitate the acquisition and use of electronic evidence, further highlighting its growing importance in legal practice (Matis, 2024)[23].

Despite its significance, electronic evidence presents substantial challenges related to authenticity and reliability, including issues of data integrity, chain of custody, and the potential for manipulation or tampering [8], [21]. The lack of standardized procedures for digital forensics further complicates its assessment, often resulting in inconsistencies in judicial evaluation and threatening legal certainty [1]. Consequently, legal systems are under pressure to adapt by incorporating more robust frameworks and forensic protocols to ensure that electronic evidence meets the necessary standards of admissibility and reliability [1], [8].

The findings of this study indicate that the interpretation of sufficient preliminary evidence becomes increasingly complex when based on electronic data, as such evidence requires careful technical validation before it can be deemed credible. In practice, however, law enforcement authorities may rely on electronic evidence without comprehensive verification due to time constraints or limited technical capacity, raising concerns about its misuse as the sole or primary basis for arrest and detention. The absence of clear legal benchmarks for evaluating electronic evidence at the preliminary stage exacerbates this issue. From a due process perspective, sufficient evidence must not only exist but also be reliable and obtained through lawful means; therefore, the use of electronic evidence must be accompanied by strict procedural safeguards to ensure compliance with fundamental legal standards.

4.3 Application of Due Process of Law in Arrest and Detention

The principle of due process of law requires that any restriction of individual liberty, including arrest and detention, be carried out in accordance with fair and lawful procedures, encompassing legal authorization, sufficient evidence, transparency, and the protection of suspects' rights. This principle is reinforced in international legal instruments such as the European Convention on Human Rights, which emphasizes the right to liberty and procedural fairness [28], as well as through judicial control mechanisms aimed at preventing arbitrary detention, as upheld by the European Court of Human Rights [16]. However, the increasing reliance on electronic evidence in criminal proceedings often lacks sufficient scrutiny, raising concerns about the adequacy of existing legal frameworks in safeguarding fundamental rights.

The findings of this study reveal that although legal frameworks formally uphold due process principles, their application in cases involving electronic evidence is not always consistent. In practice, arrests and detentions may be carried out based primarily on electronic data without adequate validation, increasing the risk of wrongful detention [17]. The effectiveness of pretrial procedures in reviewing the legality of such actions also varies across jurisdictions and often lacks robust institutional support [17]. This situation poses serious implications for individual rights, particularly the erosion of the presumption of innocence and the potential for unjust detention due to overreliance on unverified digital evidence [29].

Furthermore, the technical nature of electronic evidence creates an imbalance between law enforcement authorities and suspects, as individuals may lack the expertise or resources to challenge complex digital data effectively. This limitation restricts the exercise of procedural rights and highlights the need for greater transparency, access to independent expertise, and stronger procedural safeguards. Judicial oversight remains a crucial mechanism for ensuring due process; however, courts themselves may face difficulties in assessing electronic evidence due to its technical complexity, which can weaken the effectiveness of judicial review as a safeguard against potential abuses.

4.4 Challenges in Ensuring the Reliability of Electronic Evidence

One of the key findings of this research is the significant challenge in ensuring the reliability of electronic evidence, particularly in relation to data authenticity, data integrity, chain of custody, and the need for specialized technical expertise in digital forensics. Determining whether electronic data is genuine and free from alteration, ensuring that it remains unchanged from collection to courtroom presentation, and maintaining a clear, documented chain of custody are critical requirements that are often difficult to guarantee. These challenges directly affect the application of due process, as unreliable or improperly handled electronic evidence may render any arrest or detention based on it unlawful, especially in the absence of standardized procedures for handling digital evidence.

Furthermore, the risks associated with cyber manipulation, hacking, and unauthorized data access raise serious concerns about the credibility of electronic evidence in criminal proceedings. Without robust procedural and technical safeguards, there is a substantial risk that individuals may be wrongfully accused or detained based on compromised or tampered data. This highlights the urgent need for stronger legal standards and forensic protocols to ensure that electronic evidence is both reliable and consistent with the principles of due process of law.

4.5 Normative Evaluation of Legal Frameworks

From a normative legal perspective, the current legal framework provides a general basis for recognizing electronic evidence but lacks detailed provisions governing its use in coercive measures such as arrest and detention, creating a gap between legal recognition and practical implementation. The analysis indicates that existing regulations tend to focus primarily on the admissibility of electronic evidence in court rather than its role in the preliminary stages of criminal proceedings. Consequently, there is insufficient guidance on how electronic evidence should be evaluated before being used to justify arrest or detention, which may lead to inconsistencies and potential risks to due process.

This gap highlights the urgent need for clearer and more comprehensive legal standards, including specific criteria for determining the sufficiency of electronic evidence, mandatory forensic verification procedures, clear guidelines on lawful data acquisition, and strengthened judicial oversight mechanisms. By reinforcing these aspects, the legal system can better ensure that the use of electronic evidence aligns with due process principles, enhances legal certainty, and protects individuals from arbitrary or unjust actions.

4.6 Implications for Legal Reform and Practice

The findings of this study have significant implications for both legal reform and law enforcement practice. There is a clear need to develop comprehensive regulations that specifically address the use of electronic evidence in arrests and detentions, integrating both legal and technical standards to ensure reliability and accountability. In addition, capacity building for law enforcement and judicial institutions is essential, including training in digital forensics, a deeper understanding of electronic evidence, and stronger awareness of due process requirements. Without such capacity, the risk of misinterpretation or misuse of electronic evidence remains high.

Furthermore, the role of independent experts should be strengthened to provide objective and professional assessments of electronic evidence, thereby helping to balance the position between prosecution and defense and ensuring fairer legal proceedings. Ultimately, public trust in the criminal justice system depends on the consistent and transparent application of due process. Ensuring that electronic evidence is used responsibly, accurately, and in accordance with legal standards is crucial to maintaining this trust in the digital era.

5. CONCLUSION

This study demonstrates that the integration of electronic evidence into criminal proceedings presents both opportunities and challenges for the application of due process of law. While electronic evidence enhances the effectiveness of law enforcement in addressing modern crimes, its use as a basis for arrest and detention must be carefully regulated to prevent violations of fundamental rights. The findings indicate that existing legal frameworks have not fully accommodated the complexities of electronic evidence, particularly at the preliminary stages of criminal proceedings. The absence of clear standards for determining sufficient evidence, combined with technical challenges in verifying digital data and imbalances in technical knowledge between law enforcement and suspects, creates a risk of arbitrary or unjustified arrests and detentions, thereby undermining fairness in the legal process.

To address these challenges, it is essential to strengthen the legal and institutional frameworks governing electronic evidence by establishing clear procedural standards, enhancing the capacity of law enforcement and judicial institutions, and ensuring effective oversight mechanisms. Such improvements would enable the criminal justice system to better balance the demands of effective law enforcement with the protection of individual rights. Ultimately, the principle of due process of law must remain a central foundation in the use of electronic evidence, ensuring that technological advancements are utilized to support justice without compromising fundamental legal protections.

REFERENCES

[1] D. Fernando, D. Heniarti, and C. Zakaria, “Transformasi Alat Bukti Elektronik Menggunakan Digital Forensik Dalam Pembaharuan Hukum Acara Pidana,” *J. Justiciabelen*, vol. 5, p. 60, 2025.

[2] A. Khalaf, “Digital forensics and legal guarantees for the accused in an electronic environment,” *Al-rafidain Law J.*, vol. 27, no. 92, pp. 192–216, 2025.

[3] M. Elshobake and A. Sakka, “Legal Implications of Emerging Technologies in Criminal Investigations: Current Challenges and Catalysts for Change,” *Int. J. Soc. Sci. Res.*, vol. 12, p. 263, Sep. 2024, doi: 10.5296/ijssr.v12i2.21965.

[4] A. H. Mustafa, “The Future of Criminal Law in the Age of Electronic Crimes and Artificial Intelligence.,” *Pakistan J. Life Soc. Sci.*, vol. 22, no. 2, 2024.

[5] J. O. S. Matthew N. O. Sadiku, Paul A. Adekunte, “Digital Forensics for Law Enforcement,” vol. 9, no. 4, 2025, [Online]. Available: http://www.milwforensics.com/PrivateInvestigatorReviews-computerInvestigationsforPolice

[6] A. Sukmasari, W. Frederik, M. E. Kalalo, and M. H. Soepeno, “Application Of Electronic Evidence as Extension of Legal Civil Evidence Divorce Cases in Indonesia,” *Int. J. Law, Environ. Nat. Resour.*, vol. 4, no. 1, pp. 1–14, 2024.

[7] Y. Irianto, “Judicial Adaptation to Digital Evidence in the Era of Cyber Governance,” *Formosa J. Sci. Technol.*, vol. 4, no. 9, pp. 3015–3030, 2025.

[8] A. Suryana and M. S. Sakmaf, “Can Electronic Evidence Constitute Sufficient Grounds for Criminal Liability?,” *Jihk*, vol. 7, no. 1, pp. 587–601, 2025.

[9] K. Manurung and B. Harefa, “The Validity of Electronic Evidence and Its Relation to Personal Data Protection,” *J. Daulat Huk.*, vol. 7, p. 455, Dec. 2024, doi: 10.30659/jdh.v7i4.41815.

[10] R. A. E. Calixto, “O devido processo legal,” *Rev. Eletrônica da Fac. Direito Fr.*, vol. 11, no. 2, pp. 233–262, 2016.

[11] M. Luisi, “O PRINCÍPIO DO DEVIDO PROCESSO LEGAL,” 2010. [Online]. Available: https://api.semanticscholar.org/CorpusID:170362482

[12] M. D. Bayles, “Procedural Due Process,” in *Philosophical Dimensions Of The Constitution*, Routledge, 2019, pp. 206–221.

[13] E. Sargeant, J. Barkworth, and N. Madon, “Procedural Justice in the Criminal Justice System,” 2020. doi: 10.1093/acrefore/9780190264079.013.635.

[14] I. C. de Almeida Teles, “O princípio do devido processo legal: breves comentários,” *República Fed. do Bras.*, p. 208, 2021.

[15] A. Safinatunnajah, M. Ali, and P. Teeraphan, “Compliance of the Subjective Terms of Detention in Criminal Procedure with International Covenant on Civil and Political Rights,” *Lex Publica*, vol. 9, no. 2, pp. 88–101, 2022.

[16] R. Brander and A. Pickup, “Arrest and Detention,” 2009, pp. 157–184. doi: 10.1093/oso/9780199214419.003.0007.

[17] S. P. Indraswari, R. Chan, and A. Lee, “Effectiveness of Pretrial in Testing the Legality of Arrest and Detention,” *Rechtsnormen J. Law*, vol. 3, no. 2, pp. 146–157, 2025.

[18] K. Umam, A. Hadiyanto, and W. H. Sukrisno, “Pertimbangan Putusan Hakim Pra Peradilan Mengenai Sah Tidaknya Penetapan Tersangka: Considerations of Pretrial Judges’ Decisions Regarding The Validity of Suspect Determinations,” *J. Jurid.*, vol. 3, no. 2, pp. 169–184, 2025.

[19] E. Y. González Kow and E. E. Pozo Cabrera, “La orden de detención con fines investigativos y su incidencia en el debido proceso.,” *Reli. Rev. Ciencias Soc. y Humanidades*, vol. 9, no. 42, 2024.

[20] V. V Petryk, “The use of electronic evidence in criminal proceedings: issues of collection, verification, and evaluation,” *Uzhhorod Natl. Univ. Herald. Ser. Law*, 2025, [Online]. Available: https://api.semanticscholar.org/CorpusID:277426067

[21] H. O. Abdullah, M. Maqsood, and A. Nadeem, “Digital Evidence in Criminal Proceedings: Legal Standards, Chain of Custody, and Evidentiary Reliability in The Digital Era,” *Res. J. Soc. Aff.*, vol. 3, no. 5, pp. 795–805, 2025.

[22] О. Д. Квашук, “Використання електронних доказів у кримінальному провадженні,” *Центральноукраїнський вісник права та публічного управління*, no. 2, pp. 50–56, 2025.

[23] M. Jakub, “Certain aspects of criminal evidence and digital evidence,” 2024.

[24] A. Brīvers, “UNDERSTANDING OF ELECTRONIC EVIDENCE, ITS ACQUISITION AND STRENGTHENING IN CRIMINAL PROCEEDINGS,” in *INDIVIDUAL. SOCIETY. STATE. Proceedings of the International Student and Teacher Scientific and Practical Conference*, 2021, pp. 156–162.

[25] D. S. R. Dhumillah, "The Stand Of Electronic Evidence In Cyber Crime Law Enforcement In Indonesia," *Eduvest-Journal Univers. Stud.*, vol. 4, no. 9, pp. 7549–7559, 2024.
[26] A. Sidabutar, R. Risdalina, and I. Kumalasari, "Evidence of Criminal Acts in the Field of Electronic Information and Transactions in Review of Law No. 19 of 2016 concerning Electronic Information and Transactions," *Enrich. J. Multidiscip. Res. Dev.*, vol. 2, no. 2, pp. 60–65, 2024.
[27] S. M. Giordano, "Electronic evidence and the law," *Inf. Syst. Front.*, vol. 6, no. 2, pp. 161–174, 2004.
[28] C. Gearty, "The Rights to Liberty and Due Process," *Civil Liberties*. Oxford University Press, p. 0, Sep. 13, 2007. doi: 10.1093/oso/9780199236169.003.0006.
[29] D. Vizdoaga, "Individual Freedom from the Perspective of Detention and the Principle of Proportionality," *Rev. Institutului Natl. Justitiei*, p. 9, 2022.