



REGULATION OF ELECTRONIC DATA AND PERSONAL DATA IN INDONESIAN CRIMINAL PROCEDURE LAW

Arif Budiman, Sarwo Waskito, Kunia Wijaya

Universitas Sunan Giri Surabaya

correspondence: sarwowaskito68@gmail.com

Abstract

This research analyzes the relationship between electronic data and personal data in law enforcement and examines the harmonization of regulations between the Personal Data Protection Law and the Electronic Information and Transactions Law in the context of seizing electronic evidence. This normative legal research employs statutory and conceptual approaches using primary, secondary, and tertiary legal materials analyzed qualitatively. The findings indicate that electronic data and personal data are closely interconnected in law enforcement, yet pose significant privacy protection challenges, particularly in seizure procedures that often encompass irrelevant information. Fulfilling the authenticity, integrity, and reliability requirements for electronic evidence faces technical and legal obstacles. This research finds that implementing the principles of minimality, transparency, and accountability in seizing electronic evidence is essential to balance law enforcement needs with privacy rights protection. Harmonization among relevant laws still encounters legal gaps, including the lack of specific guidelines, weak oversight, and inadequate sanctions. Standardization of procedures, capacity building for law enforcement officers, and comprehensive technical guidelines are required to create a fair balance in the digital era.

Keywords: electronic data, personal data, seizure, evidence, privacy protection, legal harmonization, law enforcement

Introduction

The development of information technology has fundamentally transformed the data management landscape, making electronic data and personal data two elements that receive serious attention in various aspects of life, including law enforcement. This transformation is also visible in the shifting transaction patterns of society, which increasingly rely on digital systems, as reflected by the widespread use of electronic money as a substitute for cash transactions (Sinambela & Darmawan, 2022). Electronic data, as information or documents created, sent, received, stored, or processed through electronic devices, possesses characteristics different from conventional evidence. Its intangible nature, ease of modification, and capacity to be copied or transferred rapidly pose distinct challenges in the evidentiary process in court. Personal data, as information that can be identified directly or indirectly with an individual, requires special protection because it concerns individual privacy rights protected by law (Vučković & Vuckovic, 2025). The increasingly extensive role of technology across various sectors likewise drives an increased need for structured data management, including in supporting productivity and public business revenue growth (Sinambela et al., 2021). As technology continues to advance, the legal framework surrounding the management and protection of electronic and personal data must evolve to address these emerging challenges effectively.

In law enforcement practice, electronic data and personal data share a close relationship because personal data frequently constitutes a portion of electronic data managed through digital devices (Brīvers, 2023). Cybercrime cases demonstrate that electronic data in the form of user activity logs from applications can contain personal data such as names, IP addresses, or transaction details that serve as keys in identifying perpetrators or uncovering criminal motives. Cybercrime phenomena such as carding and phishing provide clear evidence that the misuse of electronic data and personal data can inflict massive losses on victims, while simultaneously affirming the importance of consistent application of the ITE Law in ensnaring perpetrators (Darmawan et al., 2025). Nevertheless, this relationship poses major challenges, particularly concerning the protection of individual privacy. The seizure of electronic evidence such as mobile phones or computers frequently encompasses information irrelevant to the case, thus risking violations of data owners' privacy if not managed in accordance with personal data protection principles. The rapid growth of electronic transactions in the digital economic system further magnifies the volume of personal data in circulation and creates potential for misuse if management is not closely monitored (Wibowo et al., 2023).

Personal data protection has become an increasingly urgent issue alongside the rising number of cybercrime cases and data breaches in Indonesia. The right to privacy is a fundamental right guaranteed in various legal instruments, both national and international. The reinforcement of clear institutional structures and orderly governance has proven to be an important factor in supporting the effectiveness of a protection system, as found in the management of institution-based financing schemes (Wiyandarini et al., 2021). In Indonesia, regulations concerning personal data protection have been established in a specific statute that provides guarantees of protection for individuals' personal data. This legislation governs the rights of data owners, including the right of access, right of correction, right to object, and right to be forgotten. The consistency of applying these regulations is also influenced by the quality of leadership within the responsible institution, as accountable and integrity-driven leadership has proven capable of creating fairer and more trustworthy governance (Mardikaningsih et al., 2022). These rights provide comprehensive protection for individuals in facing the challenges of the digital era, including in situations where their personal data becomes part of law enforcement processes (Putri & Girinatha, 2024).

The needs of law enforcement require access to electronic data as valid evidence in court. Regulatory developments in the digital finance sector similarly demonstrate that the law is constantly demanded to adapt quickly to technological changes in order to remain relevant in regulating community activities (Yuristiawan et al., 2024). Electronic data holds a significant position in uncovering legal facts, particularly in cases involving digital technology such as hacking, identity theft, online fraud, or the dissemination of hate speech. Laws in the field of information and electronic transactions stipulate that electronic information and electronic documents constitute valid legal evidence, equivalent to other evidence governed in criminal procedural law (Suryana et al., 2025). The effectiveness of a regulation is ultimately tested through its actual application in the field, as seen in the evaluation of cross-border business competition regulation implementation which highlights the need for strengthened law enforcement (Zulkarnain et al., 2024). These provisions provide a solid legal foundation for utilizing electronic data in judicial proceedings, provided such data meets standards of authenticity, integrity, and reliability.

The validity of electronic data as legal evidence depends on the fulfillment of technical and procedural requirements stipulated by law. Data authenticity ensures that the data originates from a legitimate source and has not undergone alteration since it was first created or received. Data integrity guarantees that the data is complete, undamaged, and has not been altered illegally. The reliability of

a system is generally determined by the extent to which the processes within it operate in an integrated and controlled manner, much like supply chain management principles that emphasize the importance of regularity in every stage to maintain final output quality (Barzani et al., 2022). Data reliability refers to the credibility of the electronic system used to generate, store, or process that data (Joshi et al., 2025). Aside from technical aspects, the human factor operating the electronic system also determines the reliability of the generated data, given that the level of thoroughness and responsibility of system administrators influences the quality of the resulting output (Darmawan & Mardikaningsih, 2022). Each of these technical and procedural requirements must be fulfilled cumulatively for electronic data to possess valid evidentiary force in court.

The procedure for seizing electronic evidence in criminal procedural law requires adjustments to the characteristics of electronic data, which differ from physical evidence. Seizure is an investigator's action to take over or store under their control movable or immovable objects, tangible or intangible, for the purpose of evidentiary proof in investigation, prosecution, or examination at court hearings. The implementation of such procedures demands an attitude from investigators that firmly adheres to work ethics principles, as honest and responsible actions in carrying out duties will determine the validity of the results obtained (Mardikaningsih et al., 2022). In the context of electronic evidence, seizure must pay attention to aspects of data authenticity, integrity, and security so that it can be utilized as valid evidence. Strict supervision over every stage of seizure is also necessary to prevent abuses of authority, much like the importance of firm supervisory functions in maintaining compliance with applicable regulations (Wibowo et al., 2023). Seizure procedures must likewise comply with provisions governing the validity of electronic data as legal evidence as well as personal data protection principles, such as minimality and transparency (Shulha & Kaliuzhna, 2025). Adapting seizure procedures to the characteristics of electronic data is imperative to ensure that the evidence obtained does not lose its validity due to technical errors in the data acquisition process.

There is a gap between the needs of law enforcement requiring broad access to electronic data and the protection of individual privacy rights guaranteed by personal data protection laws. This kind of tension reflects a common challenge faced by modern organizations in adapting to constantly evolving legal provisions, thus requiring good change management so that legal compliance is maintained without sacrificing other interests (Darmawan et al., 2024). Law enforcement requires electronic data as evidence to uncover crimes and prove the guilt of perpetrators in court. Personal data protection necessitates the restriction of personal data collection and use solely for legitimate and

proportional purposes. The tension between the public interest in law enforcement and the protection of individual privacy rights requires careful balancing, given that privacy rights constitute fundamental rights that cannot be derogated under any circumstances. Similar dynamics are also apparent in other sectors experiencing changes due to digitalization, where regulatory adjustments are a necessity so that the benefits of technology can be felt without diminishing protection against individual rights, as seen in shifts in public preferences toward electronic payment instruments (Sinambela & Darmawan, 2022).

This research aims to analyze the relationship between electronic data and personal data in law enforcement as well as examine the harmonization between personal data protection regulations and electronic information and transaction regulations in the context of seizing electronic evidence. This research also aims to identify challenges in implementing electronic evidence seizure procedures and formulate recommendations to create a balance between law enforcement needs and the protection of individual privacy rights. This research is expected to contribute conceptual thinking toward the refinement of the legal framework governing the use of electronic data as evidence and personal data protection in the criminal justice process in Indonesia to create a legal system that is fair and responsive to technological developments.

Method

This research employs a normative legal research method using statutory and conceptual approaches. The statutory approach is conducted by examining provisions in Law Number 27 of 2022 concerning Personal Data Protection, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, as well as the Criminal Procedure Code. The conceptual approach is utilized to analyze legal concepts related to electronic data, personal data, seizure, and evidence in criminal procedural law to gain a comprehensive understanding of the relationship between personal data protection regulations and electronic information and transaction regulations.

The legal materials used in this research consist of primary legal materials covering laws and regulations in the fields of personal data protection, electronic information and transactions, and criminal procedural law (Sidabutar et al., 2024). Secondary legal materials take the form of literature, journal articles, and legal doctrines relevant to the research topic, alongside tertiary legal materials such as legal dictionaries and encyclopedias. Data collection techniques are carried out through literature studies by systematically inventorying, classifying, and analyzing legal materials. Data analysis is

performed qualitatively using grammatical interpretation and systematic interpretation methods to capture the meaning and purpose of electronic data and personal data regulations within legislation, as well as to formulate legal arguments regarding the harmonization between personal data protection and law enforcement in the seizure of electronic evidence.

Result and Discussion

Relationship between Electronic Data and Personal Data in Law Enforcement in the Digital Era

The advancement of information technology has brought major changes in data management, making electronic data and personal data two essential elements that frequently become the center of attention in law enforcement. Electronic data, as defined in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, is information or documents created, sent, received, stored, or processed through electronic devices. This data encompasses various formats such as text, images, audio, video, or a combination of these elements. The Information and Electronic Transactions Law stipulates that electronic data can be used as valid evidence in court provided it fulfills the requirements of integrity, authenticity, and accuracy as regulated in Article 5 and Article 6 (Sidabutar et al., 2024). In law enforcement, electronic data is crucial for uncovering facts, particularly in cases involving digital technology. The readiness of law enforcement officers to follow technological developments is likewise determined by their self-efficacy in adapting to technological changes within the work environment (Mardikaningsih & Darmawan, 2022). An adaptive learning process enables individuals and law enforcement institutions to adjust gradually to the continuously changing developments of electronic data (Kurniawan & Darmawan, 2021). Every law enforcement officer is required to understand the definition and scope of electronic data so that its utilization as evidence can be conducted precisely and in accordance with statutory provisions. The mastery of knowledge regarding information technology also serves as an important asset for organizations, including law enforcement agencies, to utilize electronic data optimally and on target (Darmawan, 2023).

Personal data, as regulated in Law Number 27 of 2022 concerning Personal Data Protection, is information that can be identified directly or indirectly with an individual, either independently or in combination with other information. Personal data encompasses basic information such as names, addresses, and identity numbers, as well as sensitive information such as health data, biometrics, or financial information. The vulnerability of health data as a

component of sensitive personal data is also apparent in cases of health certificate forgery, demonstrating that the misuse of personal data can carry implications for criminal law violations and professional ethics (Hartika et al., 2023). The Personal Data Protection Law divides personal data into two types, namely general personal data and specific personal data, with stricter protection applied to specific data due to its potential impact on individual privacy (Darti et al., 2025). This statute also regulates personal data management principles, such as data owner consent, transparency, accountability, and minimality in data collection and use. Access challenges and skill gaps in utilizing technology-based services similarly influence the extent to which individuals are capable of understanding and protecting their own personal data (Ramle & Mardikaningsih, 2022). Legal protection for consumers in online buying and selling transactions likewise emphasizes the importance of managing personal data securely, given that such data frequently constitutes a part of electronic transaction processes (Rezkiyanti & Wahyudi, 2025). The classification of personal data into general and specific data determines the level of protection that must be applied in every data management process by any party whatsoever, including law enforcement officers. Changing remote working patterns involving the intensive use of employee personal data further adds to the complexity of maintaining individual psychological well-being and privacy within the work environment (Darmawan, 2023).

Electronic data and personal data share a close relationship because personal data frequently constitutes a portion of electronic data managed through digital devices. In cybercrime cases, electronic data in the form of application user activity logs can contain personal data such as names, IP addresses, or transaction details. This personal data often serves as a key in identifying perpetrators or uncovering criminal motives (Samantaray & Azeez, 2024). Criminological analysis of law enforcement in human trafficking cases likewise demonstrates that the success in uncovering criminal perpetrators depends heavily on precision in tracing data trails, including personal data stored within electronic systems (Lukmantara et al., 2022). This relationship poses major challenges, particularly concerning privacy protection. The risk of personal data misuse is also apparent in technology finance-based online lending practices, making legal risk mitigation regarding data management an important concern for both service providers and users (Sahid et al., 2023). In the seizure of electronic evidence such as mobile phones or computers, the data contained therein frequently encompasses information irrelevant to the case, thereby creating the risk of privacy violations if such data is not managed in accordance with the principles regulated in the Personal Data Protection Law. In handling serious crimes, the existence of strong

evidence, including electronic data, becomes a determining factor for the effectiveness of law enforcement against perpetrators (Ferdinanta et al., 2024). Narcotics abuse practices similarly constitute one of the cases utilizing the seizure of electronic devices as part of evidentiary efforts, making proper data management crucial so that legal processes proceed in accordance with rules (Prabowo et al., 2024). The close linkage between electronic data and personal data requires law enforcement officers to apply selective and proportional seizure procedures to protect the privacy rights of individuals unrelated to the case.

The Personal Data Protection Law and the Information and Electronic Transactions Law provide complementary guidelines for regulating the use of personal data in law enforcement. Flexible institutional structures are considered capable of enhancing an organization's capacity, including law enforcement institutions, in adapting to regulatory dynamics and continuously changing technological developments (Darmawan & Mardikaningsih, 2023). The Personal Data Protection Law stipulates that personal data collected for legal purposes may only be used in accordance with the purpose of such data collection. The principle of good faith applicable in the execution of an agreement can likewise be applied to the use of personal data, namely that data obtained for legal interests ought to be used in accordance with initial agreements and not misused for other interests (Irfansyah et al., 2024). The Information and Electronic Transactions Law establishes technical standards to ensure the integrity and authenticity of electronic data to be utilized as evidence (Jyoti, 2025). Both statutes strive to balance the needs of law enforcement with the protection of individual privacy rights. Cross-border payment transaction regulations similarly demonstrate how legal provisions endeavor to protect consumers while maintaining certainty in data management involving cross-jurisdictional parties (Rahman et al., 2024). In cases of electronic evidence seizure in cybercrime investigations, relevant personal data often serves as important evidence, yet without clear procedures to separate relevant data from irrelevant data, the risk of privacy violations remains present. Criminal law enforcement against environmental pollution perpetrators serves as one example of how specific regulations are required so that action against a violation can be executed precisely on target, much like the regulation of personal data and electronic data (Mahmud et al., 2023). Synergy between these two statutes serves as the legal foundation for law enforcement officers in carrying out investigative duties without neglecting the protection of citizens' privacy rights.

The application of the principles of transparency, accountability, and minimality in data collection and use becomes crucial to ensure that individual rights remain respected, while simultaneously enabling law enforcement to run effectively and fairly. With a robust legal framework, these challenges can be

addressed so that a balance is created between privacy protection and law enforcement needs in the digital era. There are several rights to privacy regulated in the Personal Data Protection Law, namely the right of access, right of correction, right to object, and the right to be forgotten. The role of advocates in the judicial system contributes to strengthening legal protection for individuals, including in assisting personal data owners whose rights are impacted during law enforcement processes (Jayadi et al., 2025). The rights regulated in the Personal Data Protection Law provide comprehensive protection for individuals in facing the challenges of the digital era, including in situations where their personal data becomes part of law enforcement processes. Efforts to fulfill rights and legal protection for vulnerable groups, such as elderly inmates, affirm that respect for individual rights must still be maintained even while someone is undergoing legal processes, much like the privacy rights protection principle regulated for personal data owners (Pamungkas et al., 2025).

Position of Electronic Data in Criminal Procedural Law and Challenges of Its Application in the Digital Era

The Information and Electronic Transactions Law establishes provisions concerning the validity of electronic data as legal evidence. Article 5 paragraph (1) of the Information and Electronic Transactions Law states that electronic information and electronic documents constitute valid legal evidence, equivalent to other evidence governed in the Criminal Procedure Code. This provision provides a solid legal foundation for utilizing electronic data in trial proceedings, particularly in cases involving cybercrimes, electronic contract violations, or other criminal offenses related to information technology. The application of such legal provisions demands the ability to balance the rapid pace of technological development with considerations of human values, ensuring that the resulting rules do not merely follow changing times but also remain grounded in the principles of justice (Darmawan, 2023a). For electronic data to be admissible in court, Article 6 of the Information and Electronic Transactions Law stipulates the requirements that must be met, namely authenticity, integrity, and reliability of the data (Manasa et al., 2025). Every piece of electronic data submitted as evidence is required to fulfill these three prerequisites in order to possess binding legal force at trial. The firmness of criminal rule enforcement against violations related to technology utilization across various fields demonstrates that the law must be applied consistently so that applicable norms genuinely provide a deterrent effect and certainty for the community (Noor et al., 2023).

Authenticity refers to the ability to ensure that the data has not undergone alteration since it was first created or received. Data authenticity can be proven

through electronic signatures or other authentication mechanisms. Integrity refers to the condition of data being complete, undamaged, and unaltered illegally, which can be verified using technologies such as hashing (Mohan et al., 2024). The assessment of elements of a legal act, as seen in the application of money laundering criminal offense elements in Indonesian jurisprudence, affirms that every evidentiary element must be carefully examined before it can serve as the basis for a verdict (Rusianto et al., 2023). Reliability refers to the credibility of the electronic system used to generate, store, or process that data, which must be operated securely and in accordance with standards. User trust in data security on digital platforms similarly influences the credibility of the electronic system itself, as well-maintained privacy rights will encourage user compliance in submitting accurate data (Oluwatosin, 2024). The requirements of authenticity, integrity, and reliability serve as essential instruments to prevent the misuse or manipulation of electronic data in legal processes.

In cases of defamation via social media, screenshots of conversations or posts are frequently submitted as evidence. For this evidence to be admissible, the party submitting the evidence must ensure that the data meets the standards of authenticity and integrity regulated by the Information and Electronic Transactions Law. The resolution of speech cases in the digital space does not actually always have to end in criminal prosecution proceedings, as a restorative justice approach can serve as an alternative resolution for such matters based on normative studies of the Information and Electronic Transactions Law and the Criminal Code (Rianto et al., 2023). Provisions within the Information and Electronic Transactions Law also provide a legal basis for the seizure of electronic evidence by law enforcement officers (Juliharto, 2025). The right to recovery for crime victims, including public understanding of the right to restitution, forms an important part of a fair legal process so that the losses experienced by victims also receive attention, rather than focusing solely on punishing the perpetrator (Prasetyo et al., 2024). This seizure must be carried out in accordance with procedures stipulated in the Criminal Procedure Code and by observing personal data protection principles regulated in the Personal Data Protection Law (Ekowati et al., 2025). The restorative justice approach that spares perpetrators from severe criminal sanctions also needs to consider social acceptance post-legal process, much like the issues faced by former inmates in rebuilding their civic relationships amidst society (Rizaldy et al., 2023). The fulfillment of data authenticity and integrity standards in defamation cases determines whether or not such screenshots can be accepted as valid evidence in court.

The rights guaranteed in the Personal Data Protection Law and the Information and Electronic Transactions Law provide comprehensive protection

for individuals in facing the challenges of the digital era. The Personal Data Protection Law emphasizes the importance of the right to privacy and personal data protection, while granting digital rights such as access, correction, objection, and the right to be forgotten. Awareness of these digital rights is closely related to citizen participation in state life, as citizens who understand their rights and obligations tend to be more active in overseeing the implementation of legal rules, including those governing the digital realm (Rojak et al., 2021). The Information and Electronic Transactions Law ensures that electronic data can be used as valid legal evidence, provided it meets the standards of authenticity, integrity, and reliability. The responsibility for maintaining data reliability and security also rests with digital platform providers, as seen in the obligation of digital marketing platforms to conduct business practices that do not harm other parties (Negara et al., 2024). Both of these statutes reflect government efforts to create a legal system responsive to technological developments, while ensuring that individual rights remain protected. The gap in public understanding of various regulations protecting their interests, as seen in public attitudes toward the distribution of non-compliant products, indicates that law enforcement must be accompanied by adequate information dissemination to the community (Purwanto et al., 2025). The implementation of rights guaranteed in both laws requires better supervision and legal awareness to ensure their effective execution amidst society. This effort must also pay attention to the gap in adaptive capabilities among community groups toward digital technology, including older workers who require mentoring so they are not left behind in utilizing digital systems within the work environment (Darmawan, 2023). The principle of information openness and consumer rights protection applicable across various business sectors, including the obligation of business actors to provide truthful information regarding distributed products, reflects that the protection of individual rights is not limited solely to the realm of personal data, but applies equally to other aspects of social life (Purwanto et al., 2023).

Relevance and Complexity of Electronic Evidence Seizure in Cybercrime Cases

The seizure of electronic evidence in Indonesia's law enforcement constitutes a crucial step in uncovering crimes, particularly in the digital era. Within criminal procedural law, seizure procedures are governed by the Criminal Procedure Code, which serves as a guideline for law enforcement officers to conduct seizures lawfully and in accordance with the law. The legal framework governing business practices across various sectors similarly exhibits a parallel pattern, namely the necessity for rules capable of keeping pace with changing times in order to prevent

deviations that harm other parties (Indarto et al., 2023). With the advancement of technology, the relevance and challenges of seizing electronic evidence have increasingly become a focus of attention, especially in handling cybercrime cases. The technical and legal complexities associated with the seizure of electronic evidence require a more modern and integrated approach alongside related regulations, such as the Information and Electronic Transactions Law and the Personal Data Protection Law (Suryana et al., 2025). The effectiveness of personal data protection regulations has also been tested in other sectors laden with digital transactions, where the implementation of such rules has proven to play a vital role in preventing customer data leaks (Aziz et al., 2023). Case handling involving the digital realm has likewise been directed toward resolutions that pay attention to the balance between legal certainty and recovery, as examined in normative analyses of the Information and Electronic Transactions Law and the Criminal Code (Darmawan & Negara, 2023). Every law enforcement officer is required to understand the provisions within all three regulations so that the seizure of electronic evidence can be executed lawfully and accountably. The management of large volumes of data obtained from the seizure process additionally requires appropriate analytical capabilities so that it can serve as an accurate basis for decision-making in case handling (Ali & Darmawan, 2023). The institutional capacity of law enforcement in adopting new working methods also serves as a determining factor for the success of electronic evidence seizure, given that organizational adaptation to new technology influences the institution's competitiveness in carrying out its duties (Abdullah et al., 2021).

The requirements that must be fulfilled for a seizure to be conducted based on Article 1 number 35 of Law Number 25 of 2025 concerning the Criminal Procedure Code state that seizure is an investigator's action to take over or store under their control movable or immovable objects, tangible or intangible, for the purpose of evidentiary proof in investigation, prosecution, or examination at court hearings. This definition encompasses intangible objects, meaning that electronic data possessing a digital nature is included among objects that can be seized (Supriyanto et al., 2023). This expansion of the scope of seizeable objects demands investigators to act honestly and consistently across every stage of evidence handling, much like the principle of good faith emphasized in the execution of other legal relationships (Irfansyah et al., 2024). These provisions provide a legal foundation for investigators to conduct seizures of electronic data relevant to the case being handled. The increasing workload resulting from handling large volumes of electronic data must also be balanced with attention to investigators' working conditions, as psychological well-being likewise determines thoroughness in carrying out seizure duties (Issallillah & Khayru,

2025). The recognition of intangible objects as seizure items strengthens the position of electronic data as valid evidence within the Indonesian criminal justice system. A similar principle applies equally in handling criminal cases involving child offenders, where a restorative approach and protection remain primary considerations even though the evidentiary process must still be executed lawfully (Al Haibah et al., 2024).

Electronic evidence serves as a crucial element in uncovering various cybercrime cases, such as hacking, identity theft, online fraud, or the dissemination of hate speech. Fraud cases in online transactions represent one clear example where electronic evidence plays a major role in protecting disadvantaged consumer rights (Ali et al., 2024). The development of criminal *modi operandi* has likewise expanded into the misuse of digital assets such as cryptocurrencies, which creates distinct legal loopholes in enforcement efforts (Balkista et al., 2024). Electronic evidence encompasses data stored in devices such as mobile phones, computers, servers, or cloud systems, including digital documents, emails, chat histories, or other metadata. Blockchain-based technology underlying a number of digital transactions likewise introduces new challenges in tracking and evidentiary proof, given its decentralized nature (Darmawan & da Silva, 2025). The seizure of electronic evidence holds a strategic role in proving the perpetrator's involvement in criminal acts. Disputes in electronic transactions involving product return processes further demonstrate that the responsibility of digital platforms forms an inseparable part of protecting user rights, making electronic transaction evidence a determinant in their resolution (Anugroh et al., 2023). Procedures for seizing electronic evidence require adjustments to the characteristics of electronic data, which differ from physical evidence (Azam et al., 2023). Electronic data is intangible, easily modified, and can be copied or transferred rapidly. Public legal awareness across various social issues, including those concerning the private sphere itself, affirms that strong evidence and adequate legal understanding remain absolute prerequisites in every law enforcement process (Da Silva & Khayru, 2025). Adapting seizure procedures to the characteristics of electronic data constitutes an absolute requirement to maintain the validity of evidence in court.

The seizure of electronic data must pay attention to aspects of data authenticity, integrity, and security so that it can be utilized as valid evidence in court. The utilization of data on a large scale is also prone to triggering unfair treatment toward specific individuals if not managed with the principle of caution, as found in customer data processing practices within the insurance sector (Bashori et al., 2024). This procedure must comply with regulations stipulated in the Information and Electronic Transactions Law concerning the

validity of electronic data as legal evidence. Adequate digital understanding among business actors likewise influences how consumer personal data is managed in online marketing practices, making digital literacy part of data misuse prevention efforts (Halizah & Darmawan, 2025). In handling cybercrimes, the relevance of electronic evidence seizure also involves protecting individual digital rights regulated in the Personal Data Protection Law. Ethical responsibility and compliance with legal obligations commonly demanded of business actors in maintaining their accountability are similarly relevant to apply to parties handling seized data (Darmawan, 2022a). Personal data seized from the electronic devices of perpetrators or witnesses must be processed in accordance with personal data protection principles, such as minimality and transparency (Sidabutar et al., 2024). Consumer interactions in online transactions likewise generate data footprints that possess the potential to become part of electronic evidence, making the quality of transaction data management deserving of equal attention (Darmawan, 2022b). This is important to prevent data misuse that could harm individuals not directly related to the case. The fulfillment of data authenticity, integrity, and security aspects must run concurrently with respect for the privacy rights of individuals whose data is seized during law enforcement processes.

Electronic data as evidence in law enforcement must fulfill the requirements of authenticity, integrity, reliability, relevance, and compliance with legal procedures. Data must be relevant to the legal case and obtained through lawful seizure, in accordance with provisions in the Criminal Procedure Code that mandate court permission, documentation, and notification to the owner of the goods. The constantly growing volume of data resulting from the proliferation of transactions on digital platforms further burdens the process of identifying and verifying evidence, as seen in consumer behavior patterns that tend toward spontaneous purchasing in online markets (Darmawan & Gatheru, 2021). Technical challenges such as data security, large data volumes, and a lack of technical expertise among law enforcement officers frequently hinder the fulfillment of these requirements. Such limitations in technical expertise can actually be overcome through the strengthening of knowledge and creativity among officers in managing data in the digital era, much like the importance of such capabilities for overall work productivity (Darmawan, 2023). This enhancement of knowledge must likewise be accompanied by the active involvement of officers in understanding increasingly automated working systems, ensuring that technology-based routine tasks can still be executed accurately (Darmawan, 2024a). Electronic data also frequently involves personal data, which triggers conflicts with privacy rights protected by the Personal Data Protection Law.

Changing working patterns resulting from automation similarly influence how institutions restructure work division and operational flexibility, including within institutions handling the management of seized data (Mardikaningsih, 2025). The reliance on algorithm-based systems across various digital platforms further generates new issues concerning who bears responsibility for automatically generated data, a problem that also emerges in platform-based work arrangements (Darmawan, 2024b). The validity of electronic data as evidence requires careful management, reliable technology, and adequate legal understanding so that every technical and juridical challenge can be addressed systematically. This complexity is increasingly felt in institutions operating cross-regionally, just as changing working relations due to digitalization demand governance adjustments in organizations operating across borders (Darmawan et al., 2023).

Legal Loopholes and Policy Improvements in the Seizure of Electronic Evidence to Protect Privacy Rights

The seizure of electronic evidence poses significant challenges concerning personal data protection because the electronic data seized frequently encompasses sensitive information belonging to perpetrators, victims, or third parties not directly involved in the legal case. Data leaks or the misuse of personal data within the digital finance and electronic commerce sectors indicate that the mechanisms for restoring consumer rights regarding leaked data still need to be strengthened, a condition that is similarly relevant when personal data becomes part of legal processes (Mujisulistyo et al., 2024). To manage this challenge, harmonization is required between Law Number 27 of 2022 concerning Personal Data Protection and Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions (Lutrianto, 2025). Fairness and accountability in electronic transactions likewise demand clarity of rules regarding the validity of digital data as well as adequate dispute resolution mechanisms, ensuring that the interests of consumers and parties whose data is processed remain protected (Purnomo et al., 2025). This harmonization aims to create a balance between law enforcement needs and the protection of individual privacy rights. Regulatory uncertainty frequently constitutes a distinct challenge for parties required to adjust their legal compliance strategies, much like the challenges faced by law enforcement officers in applying electronic

evidence seizure rules (Mardikaningsih & Darmawan, 2021). Without adequate harmonization, the process of seizing electronic evidence risks triggering violations of privacy rights protected by law. Legal certainty at the final stage of a criminal process, for instance regarding verdicts possessing final legal force, affirms the importance of procedural clarity at every stage of law enforcement, including during the electronic evidence seizure stage (Rawi et al., 2026).

The Personal Data Protection Law establishes a number of principles that must be adhered to in personal data management, including when such data becomes evidence in legal processes. The development and application of responsible technology demand an approach that pays attention to ethical and fairness aspects from the design stage onward, including within systems utilized to manage personal data (Radjawane & Mardikaningsih, 2022). Three main principles relevant to the seizure of electronic evidence are minimality, transparency, and accountability. The principle of minimality emphasizes that personal data collection and use must be limited to matters strictly relevant to legitimate legal objectives (Khalaf & Khalaf, 2025). The professional integrity of law enforcement officers serves as an essential element in ensuring that such principles are genuinely applied consistently rather than merely functioning as procedural formalities (Saktiawan et al., 2021). In the seizure of electronic evidence, the principle of minimality means that seized data must be selective, encompassing the information necessary for case evidentiary proof. A similar issue is also apparent in the dissemination of traffic accident victim information through digital media, affirming that the widespread distribution of personal data without clear boundaries can generate ethical as well as legal problems (Muhammad et al., 2023). This principle aims to protect individuals' personal data from unnecessary exposure. The tendency of business actors to utilize user data broadly within social media-based promotional strategies likewise serves as a reminder that personal data collection ought to remain limited to reasonable needs (Mardikaningsih & Halizah, 2024).

The principle of transparency requires law enforcement officers to provide information to data owners regarding the reasons for seizure, what data will be taken, and how such data will be utilized. Information openness also serves as an essential element in protecting parties involved

in trust-based activities such as online rotating savings and credit associations, where clear rules likewise determine participants' sense of security regarding the management of their data and funds (Negara & Darmawan, 2023). In the seizure of electronic evidence, transparency encompasses official notification to the owner of the goods and related parties as regulated in the Criminal Procedure Code. This principle is important to build public trust in the legal process. Openness and clear responses to assessments from other parties, as seen in the management of consumer reviews by business actors, demonstrate that an open attitude can strengthen the trust of interested parties in a process (Negara et al., 2021). The principle of accountability means that the party conducting the seizure bears full responsibility for the management of the seized personal data (Ruohonen, 2023). The certainty of norms and the legitimacy of rule enforcement serve as prerequisites for a provision to be implemented consistently and obeyed by those it regulates, including in the management of seized personal data (Wibisono et al., 2023). Data must be stored securely, processed in accordance with the law, and must not be misused for interests outside the legal process. If a violation of personal data protection occurs during the seizure process, the responsible party must be held accountable. The consistent application of accountability is also important so that the treatment of data owners is not influenced by certain views or assumptions that have the potential to trigger unequal treatment (Sajjapong et al., 2022).

The integration of the provisions of the Personal Data Protection Law and the Information and Electronic Transactions Law in the seizure of electronic evidence requires procedural standardization, the use of appropriate technology, law enforcement training, and the drafting of comprehensive technical guidelines. Experience in integrating a recovery approach into existing rehabilitation mechanisms indicates that successful integration depends on the readiness of the existing system to adopt new approaches consistently (Udjari et al., 2022). Procedural standardization is necessary to ensure that every seizure of electronic evidence is conducted in a uniform manner and in accordance with applicable legal provisions (Manurung & Harefa, 2024). The utilization of technology aligned with sustainability objectives similarly demonstrates that applying new technology within

a system requires work process adjustments so that its benefits can be achieved optimally (Mardikaningsih & Wardoyo, 2024a). The use of appropriate technology is required to maintain the integrity and authenticity of electronic data during the seizure and storage processes. Enhancing human resource capacity through the utilization of digital innovation becomes one of the determining factors for an organization's success in adapting to change, including changes in electronic evidence handling practices (Mardikaningsih & Wardoyo, 2024b). Law enforcement training is necessary to enhance the technical capacity and legal understanding of officers in handling electronic evidence. The application of alternative mechanisms such as diversion in handling juvenile offenders likewise shows that the integration of various criminal procedural elements requires clear technical guidelines to be executed properly (Utama et al., 2024). Each of these integration elements plays a mutually supportive role in realizing seizure procedures that protect privacy rights optimally. The survival capability of a small business in facing the pressures of change is similarly determined by the competencies it possesses, a principle that applies equally to law enforcement institutions in facing demands for changing electronic evidence handling procedures (Mardikaningsih et al., 2022).

There are legal loopholes that need to be addressed in the regulation of electronic evidence seizure, such as a lack of specific guidelines, weak supervision, and inadequate sanctions. Weaknesses in evidentiary aspects and official recording, as seen in land disputes based on private sale and purchase deeds, affirm that the absence of detailed guidelines can open up room for uncertainty in legal processes (Sulani et al., 2024). The lack of specific guidelines causes law enforcement officers to lack clear references in conducting the seizure of electronic evidence. Structural obstacles within the criminal justice system similarly demonstrate that the optimization of a legal mechanism, including evidence management, requires improvements at the institutional level rather than merely technical rules alone (Saputra et al., 2024). Weak supervision has the potential to trigger the misuse of personal data during the seizure process. The effectiveness of criminal sanctions in providing a deterrent effect also depends on the consistency of their application, as found in studies regarding sanctions for criminal acts of corruption (Suhartono et al.,

2024). Inadequate sanctions reduce the deterrent effect against personal data protection violations within law enforcement processes (Manurung & Harefa, 2024). A restorative approach in resolving criminal cases can serve as an alternative to fill such gaps, particularly for violations that do not require full litigation processes (Wijaya et al., 2022). With improvements to these three legal loopholes, the Indonesian legal system can become more responsive to the challenges of the digital era, safeguard individual privacy rights, and simultaneously support a fair and transparent law enforcement process.

Harmonization between the Personal Data Protection Law, the Information and Electronic Transactions Law, and the Criminal Procedure Code in the seizure of electronic evidence represents an essential step to create a balance between personal data protection and law enforcement needs. Efforts to maintain a balance among various interests, as seen in the formulation of public policies that consider economic, social, and environmental aspects simultaneously, provide an illustration that the harmonization of legal rules also needs to consider various interrelated interests (Mardikaningsih & Hariani, 2021). The principles of minimality, transparency, and accountability must serve as the foundation in every seizure process. Protection for parties disadvantaged by a product or process failing to meet standards indicates that legal accountability needs to be proportionally assigned to parties authorized to manage such risks, a similar principle that likewise applies in the management of seized personal data (Marsal et al., 2025). The integration of the provisions of both statutes requires commitment from all related parties, including law enforcement officers, policymakers, and the community. The application of technology within a working system needs to ensure that it does not trigger unequal treatment for parties involved within it, a principle relevant as well to the application of technology in law enforcement processes (Darmawan, 2024). With proper harmonization, Indonesia's legal system can protect individual privacy rights without sacrificing law enforcement effectiveness in the digital era.

Conclusion

Electronic data and personal data share a close relationship in law enforcement, where personal data frequently forms an integral part of electronic data seized as

evidence in cybercrime cases and other criminal offenses involving digital technology. The position of electronic data as valid evidence has been recognized by the Information and Electronic Transactions Law provided it fulfills the standards of authenticity, integrity, and reliability, yet the application of these requirements in seizure practices encounters various technical and legal challenges, including intangible data characteristics, ease of modification, and large data volumes. The electronic evidence seizure procedures regulated in the Criminal Procedure Code have accommodated intangible objects as items subject to seizure, yet they are not yet fully integrated with the personal data protection principles regulated in the Personal Data Protection Law, thereby posing the risk of violating individual privacy rights if not managed with care.

Harmonization between the Personal Data Protection Law, the Information and Electronic Transactions Law, and the Criminal Procedure Code in the seizure of electronic evidence still faces legal loopholes that need to be addressed, such as a lack of specific technical guidelines, weak supervisory mechanisms, and inadequate sanctions against personal data protection violations within law enforcement processes. The application of the principles of minimality, transparency, and accountability serves as an important foundation in every seizure process to ensure that the collection and use of personal data are limited to what is relevant, conducted with clear notification, and managed with accountability. Therefore, the standardization of seizure procedures, the use of reliable technology to maintain data integrity, continuous training for law enforcement officers, and the drafting of comprehensive technical guidelines are necessary as strategic steps to create a balance between law enforcement effectiveness and the protection of individual privacy rights in the digital era. With proper harmonization and commitment from all related parties, Indonesia's legal system can become more responsive to technological developments without sacrificing citizens' fundamental rights.

References

- Abdullah, M. H. A. B., Gardi, B., & Darmawan, D. 2021. Innovation in Human Resource Management to enhance Organizational Competitiveness in the Era of Globalization. *Journal of Social Science Studies*, 1(1), 51–58.
- Al Haibah, M. F. F., Hardyansah, R., & Saktiawan, P. 2024. Implementation of the Juvenile Justice System in the Case of Child Murder Offenders: Restorative, Protection, and Social Reconstruction Principles. *Studi Ilmu Sosial Indonesia*, 4(2), 21-40.

- Ali, E. M., Dirgantara, F., & Darmawan, D. 2024. Legal Protection of Consumers in Online Transactions: A Case Study of Online Fraud in Indonesia. *International Journal of Service Science, Management, Engineering, and Technology*, 6(3), 27-38.
- Ali, R., & Darmawan, D. 2023. Big Data Management Optimization for Managerial Decision Making and Business Strategy. *Journal of Social Science Studies*, 3(2), 139-144.
- Anugroh, Y. G., Hardiyansah, R., Darmawan, D., Khayru, R. K., & Putra, A. R. 2023. Consumer Protection and Responsibilities of E-commerce Platforms in Ensuring the Smooth Process of Returning Goods in COD Transactions. *Journal of Social Science Studies*, 3(2), 89-94.
- Azam, H., Dulloo, M. I., Majeed, M. H., Wan, J. P. H., Xin, L. T., & Sindiramutty, S. R. 2023. Cybercrime Unmasked: Investigating Cases and Digital Evidence. *International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence*, 2(1). <https://doi.org/10.54938/ijemdcrai.2023.02.1.255>
- Aziz, A., Darmawan, D., Khayru, R. K., & Wibowo, A. S. 2023. Effectiveness of Personal Data Protection Regulation in Indonesia's Fintech Sector. *Journal of Social Science Studies*, 3(1), 23-28.
- Balkista, D. N., Hardiyansah, R., Darmawan, D., Saktiawan, P., & Saputra, R. 2024. Legal Gaps and Enforcement Challenges in Addressing Digital Fraud Involving Cryptocurrencies as Tradable Commodities in Indonesia. *Journal of Science, Technology and Society (SICO)*, 5(2), 33-44.
- Barzani, L. A., Darmawan, D., & Zulkarnain, M. A. B. 2022. The Application of Sustainable Supply Chain Management Principles in the Manufacturing Industry to Improve Operational Performance and Corporate Social Responsibility. *International Journal of Service Science, Management, Engineering, and Technology*, 1(1), 38-45.
- Bashori, B., Hardiyansah, R., & Darmawan, D. 2024. Legal Analysis of Big Data and Analytics in Preventing Discrimination and Protecting Insurance Customers. *Journal of Social Science Studies*, 4(1), 185-192.
- Brīvers, A. 2023. Understanding of electronic evidence, its acquisition and strengthening in criminal proceedings. *Indivīds. Sabiedrība. Valsts*, 156-162. <https://doi.org/10.17770/iss2021.6913>
- Da Silva, E. B., & Khayru, R. K. 2025. Marital Rape in the Perspective of Legal Consciousness and Social Norms. *Studi Ilmu Sosial Indonesia*, 5(1), 359-380.
- Darmawan, D. 2022. Environmental Accountability through Business Ethics, Responsibility, Morals and Legal Obligations. *Bulletin of Science, Technology and Society*, 1(2), 1-6.
- Darmawan, D. 2022. Salesperson Interaction Quality and Consumer Decisions in Online Transactions. *Journal of Social Science Studies*, 2(2), 91-98.
- Darmawan, D. 2023. Innovation Culture That Balances Technological Speed with the Depth of Humanistic Thought. *International Journal of Service Science, Management, Engineering, and Technology*, 4(1), 47-54.

- Darmawan, D. 2023. Knowledge Management as a Source Of Competitive Advantage in Information Technology Companies. *International Journal of Service Science, Management, Engineering, and Technology*, 3(2), 44–50.
- Darmawan, D. 2023. Measuring Employee Productivity in the Digital Era by Considering Human Creativity and Innovation. *International Journal of Service Science, Management, Engineering, and Technology*, 4(3), 47–53.
- Darmawan, D. 2023. Social Inclusion for Older Workers in the Implementation of Digital Technology within Organizations. *International Journal of Service Science, Management, Engineering, and Technology*, 4(2), 44–51.
- Darmawan, D. 2023. The Concept Of Remote Work: A Literature Review on its Impact on Work Dynamics, Psychological Well-Being, and Social Relationships Among Employees. *International Journal of Service Science, Management, Engineering, and Technology*, 3(3), 49–55.
- Darmawan, D. 2024. Algorithmic Management in Digital Platforms and Work Dehumanization in the Gig Economy. *Studi Ilmu Sosial Indonesia*, 4(2), 183-216.
- Darmawan, D. 2024. Strategies for Enhancing Employee Knowledge and Engagement in Automated Routine Work. *International Journal of Service Science, Management, Engineering, and Technology*, 6(1), 65–71.
- Darmawan, D. 2024. The Role of Technology in Promoting or Hindering Gender Equality in the Workplace. *International Journal of Service Science, Management, Engineering, and Technology*, 6(2), 67–73.
- Darmawan, D., & da Silva, B. D. S. 2025. Blockchain as an Instrument of Decentralized Social Order and Democratic Reconfiguration. *Bulletin of Science, Technology and Society*, 4(1), 11-18.
- Darmawan, D., & Gatheru, J. 2021. Understanding Impulsive Buying Behavior in Marketplace. *Journal of Social Science Studies*, 1(1), 11-18.
- Darmawan, D., & Mardikaningsih, R. 2022. The Role of Positive Psychological Factors in Enhancing Employee Engagement and Commitment to Work Tasks. *International Journal of Service Science, Management, Engineering, and Technology*, 1(2), 37–45.
- Darmawan, D., & Mardikaningsih, R. 2023. The Role of Flexible Organizational Structures in Enhancing Corporate Adaptability to Environmental Dynamics. *International Journal of Service Science, Management, Engineering, and Technology*, 3(1), 44–49.
- Darmawan, D., & Negara, D. S. 2023. The Application of Restorative Justice in Resolving Speech Cases in the Digital Space: A Normative Analysis of the Electronic Information and Transactions Law and the Criminal Code. *Journal of Social Science Studies*, 3(1), 295-306.
- Darmawan, D., Gardi, B., & Da Silva, E. B. 2023. Exploration of Changes in Management and Employee Work Relations in Multinational Companies in the Era of Literacy-Based Digitalization. *Journal of Science, Technology and Society (SICO)*, 4(2), 43–54.

- Darmawan, D., Hardyansah, R., & Marzuki, A. A. A. 2025. Analysis of The ITE Law and Criminal Acts of Carding and Phishing in Indonesia. *Jurnal Bina Mulia Hukum*, 10(1), 1-17.
- Darmawan, D., Hardyansah, R., Sulani, S., Marsal, A. P., & Da Silva, E. B. 2024. Change Management and Legal Compliance in Modern Organizations. *International Journal of Service Science, Management, Engineering, and Technology*, 6(3), 11-16.
- Darti, A., & Marnija, M. 2025. The urgency of protecting sensitive data is reflected in Article 4(2) of Law No. 27/2022 on Personal Data Protection. *Journal Equity of Law and Governance*, 7(1), 10–21. <https://doi.org/10.22225/elg.7.1.11938.10-21>
- Ekowati, E., Fatorina, F., Mukhtarzain, A. A., & Asriana, A. Y. 2025. Keabsahan Alat Bukti Surat Berupa Hasil Cetak Media Sosial dalam Perspektif Hukum Acara Perdata. *As-Syar'i: Jurnal Bimbingan Dan Konseling Keluarga*, 7(2). <https://doi.org/10.47467/as.v7i2.8573>
- Ferdinanta, A. S. I., Saputra, R., & Darmawan, D. 2024. The Effectiveness of Death Penalty as an Effort to Counter Serious Crimes: A Literature Review. *Bulletin of Science, Technology and Society*, 3(1), 52-62.
- Halizah, S. N., & Darmawan, D. 2025. Kompetensi Digital Marketing dan Peran Literasi Digital pada Wirausaha Muda. *Jurnal Ekonomi Dan Bisnis*, 15(1), 81-96.
- Hartika, Y., Saputra, R., Pakpahan, N. H., Darmawan, D., & Putra, A. R. 2023. A Study on the Falsification of Health Certificates: Perspective of Criminal Law and Professional Ethics. *Journal of Social Science Studies*, 3(2), 175-180.
- Indarto, T., Negara, D. S., & Darmawan, D. 2023. Legal Frameworks for Mitigating Monopoly Practices Adverse to MSMEs in Indonesia. *Journal of Social Science Studies*, 3(1), 1-8.
- Infante, A., & Mardikaningsih, R. 2022. The Potential of Social Media as a Means of Online Business Promotion. *Journal of Social Science Studies*, 2(2), 45-49.
- Irfansyah, M. F., Darmawan, D., & Hardyansah, R. 2024. Implementation of the Principle of Good Faith in Contract Performance. *Bulletin of Science, Technology and Society*, 3(2), 51-56.
- Issalillah, F., & Khayru, R. K. 2025. Mental Health as an Organizational Construct: A Strategic Reorientation of Human Resource Management for Work Environment Design. *International Journal of Service Science, Management, Engineering, and Technology*, 8(3), 1–9.
- Jayadi, H., Saputra, R., & Dirgantara, F. 2025. The Role of Lawyers in the Judicial System: Responsibilities, Challenges and Strengthening Legal Protection. *Studi Ilmu Sosial Indonesia*, 5(2), 81-94.
- Joshi, N., Kumar, R., & Patel, P. 2025. The Role of Electronic Evidence in the Civil Case Evidence Process. *Rechtsnormen Journal of Law*, 3(1), 80–90. <https://doi.org/10.70177/rjl.v3i1.2090>
- Juliharto, V. A. 2025. The Power of Screenshot Evidence in Proving Cyber Crimes. *JIHAD: Jurnal Ilmu Hukum Dan Administrasi*. <https://doi.org/10.58258/jihad.v7i4.9988>

- Jyoti, J. 2025. Impact of the digital personal data protection act on law-enforcement investigations. *Law Identity and Development Law Review*, 3(1). <https://doi.org/10.70183/lijdlr.2025.v03.173>
- Khalaf, A. 2025. Digital forensics and legal guarantees for the accused in an electronic environment. *Al-Rafidain of Law*, 27(92), 192–216. <https://doi.org/10.33899/alaw.2025.162568.1353>
- Kurniawan, Y., & Darmawan, D. 2021. The Adaptive Learning Effect on Individual and Collecting Learning. *Journal of Social Science Studies*, 1(1), 93–98.
- Lukmantara, R. H., Suwito, S., & Darmawan, D. 2022. Criminological Perspectives on Criminal Law Enforcement in Human Trafficking Cases: A Literature Review. *Bulletin of Science, Technology and Society*, 1(3), 37–44.
- Lutrianto, I., & Al-Qasimi, H. A. S. B. M. 2025. Legal Problems of Personal Data Protection in The Digital Era in Personal Data Protection Law in Indonesia. *Global International Journal of Social Sciences*, 3(2), 345–350. <https://doi.org/10.38035/gijlss.v3i2.429>
- Mahmud, M., Darmawan, D., Khayru, R. K., Nuraini, R., & Issalillah, F. 2023. Enforcement of Criminal Law Against Perpetrators of Environmental Pollution. *International Journal of Service Science, Management, Engineering, and Technology*, 4(1), 43–46.
- Manasa, A. S., Lolong, W. R. J., & Rawung, H. B. R. 2025. Informasi Elektronik Sebagai Alat Bukti dalam Perkara Perdata di Pengadilan. *Khatulistiwa*, 5(4), 77–90. <https://doi.org/10.55606/khatulistiwa.v5i4.7482>
- Manurung, K. H., & Harefa, B. 2024. The Validity of Electronic Evidence and Its Relation to Personal Data Protection. *Jurnal Daulat Hukum*, 7(4), 455–455. <https://doi.org/10.30659/jdh.v7i4.41815>
- Mardikaningsih, R. 2025. The Deconstruction of Work and HRM Reconfiguration: Flexibility and Employer Branding in the Digital Era. *International Journal of Service Science, Management, Engineering, and Technology*, 8(2), 10–17.
- Mardikaningsih, R., & Darmawan, D. 2021. Business Sustainability Strategies in the Facing of Regulatory Uncertainty and Managerial Challenges. *Journal of Social Science Studies*, 1(2), 111–118.
- Mardikaningsih, R., & Darmawan, D. 2022. The Role of Self-Efficacy in Predicting Employee Adaptability to Technological Change in the Workplace. *International Journal of Service Science, Management, Engineering, and Technology*, 2(3), 43–55.
- Mardikaningsih, R., & Halizah, S. N. 2024. Strategi Promosi Usaha Berbasis Media Sosial pada Era Ekonomi Digital. *Jurnal Ekonomi Dan Bisnis*, 14(1), 51–66.
- Mardikaningsih, R., & Hariani, M. 2021. Realizing Sustainability in Public Policy: Building a Balance between Economy, Social, and Environment. *Journal of Social Science Studies*, 1(1), 191–196.
- Mardikaningsih, R., & Nuraini, R. 2022. Implementation of Circular Economy Principles for Sustainable Waste Management in the Industrial Sector. *International Journal of Service Science, Management, Engineering, and Technology*, 1(3), 41–47.

- Mardikaningsih, R., & Wardoyo, D. T. W. 2024. Green Technology Integration in Management for Social and Environmental Sustainability. *International Journal of Service Science, Management, Engineering, and Technology*, 6(2), 6-10.
- Mardikaningsih, R., & Wardoyo, D. T. W. 2024. The Role of Technology in Human Resource Development for Sustainability: A Literature Review on Digital Innovation. *Bulletin of Science, Technology and Society*, 3(3), 20-26.
- Mardikaningsih, R., Azizah, E. I., Putri, N. N., Alfian, M. N., & Rudiansyah, M. M. D. H. 2022. Business Survival: Competence Of Micro, Small and Medium Enterprises. *Journal of Social Science Studies (JOS3)*, 2(1), 1-4.
- Mardikaningsih, R., Halizah, S. N., Darmawan, D., Masithoh, N., & Nuraini, R. 2022. Examining the Role of Authentic Leadership in Shaping Positive Work Climate and Organizational Citizenship Behavior. *International Journal of Service Science, Management, Engineering, and Technology*, 2(1), 52-59.
- Mardikaningsih, R., Halizah, S. N., Nuraini, R., & Darmawan, D. 2022. The Role of Ethical Leadership in Shaping a Positive and Sustainable Organizational Culture. *International Journal of Service Science, Management, Engineering, and Technology*, 2(2), 48-55.
- Marsal, A. P., Darmawan, D., & Hardyansah, R. 2025. Product Liability, Defective Goods, and Consumer Compensation in Business Law. *Bulletin of Science, Technology and Society*, 4(3), 59-68.
- Mohan, C. R., Saxena, R., Thilagam, K. T., Solleti, P. K., Sivasubramanian, S., & Dharamvir. 2024. Blockchain-Based Solutions for Enhancing Data Integrity and Security. *IEEE*, 1416-1420. <https://doi.org/10.1109/ic3i61595.2024.10828945>
- Muhammad, A. I., Saputra, R., Pakpahan, N. H., Darmawan, D., & Khayru, R. K. 2023. Ethics and Legality in the Dissemination of Information on Traffic Accident Victims Through Digital Media. *Journal of Social Science Studies*, 3(2), 235-244.
- Mujisulistyo, Y. F., Darmawan, D., & Dirgantara, F. 2024. Reconstruction of the Legal Mechanism for Consumer Rights Recovery Regarding Personal Data Leaks in the Financial Technology and E-Commerce Sectors in Indonesia. *Journal of Social Science Studies*, 4(1), 75-84.
- Negara, D. S., & Darmawan, D. 2023. Digital Empowerment: Ensuring Legal Protections for Online Arisan Engagements. *Bulletin of Science, Technology and Society*, 2(2), 13-19.
- Negara, D. S., Darmawan, D., & Gardi, B. 2021. The Approach of Consumer Reviews to Product Competitiveness and Management Strategies. *Journal of Social Science Studies*, 1(2), 149-154.
- Negara, D. S., Jauhari, M. A., & Darmawan, D. 2024. Responsibilities of Digital Marketplace Platforms and Anticompetitive Assessments in Business Law. *Journal of Social Science Studies*, 4(1), 407-422.
- Noor, T., Putra, A. R., Suyuti, M., Khayru, R. K., Hariani, M., Issalillah, F., & Mardikaningsih, R. 2023. Implementation of Criminal Regulations on The Use of Hazardous Chemicals in Food Distribution. *International Journal of Service Science, Management, Engineering, and Technology*, 4(3), 13-17.

- Oluwatosin, A. 2024. Privacy Rights, Inference, and User Trust in Digital Platform Services. *Journal of Social Science Studies*, 4(1), 381-390.
- Pamungkas, D. S. P., Dirgantara, F., Saputra, R., Khayru, R. K., & Pakpahan, N. H. 2025. Efforts to Fulfill the Rights and Legal Protection of Elderly Prisoners in Correctional Institutions Through Service Reform and Strengthening the Monitoring System. *Studi Ilmu Sosial Indonesia*, 5(1), 45-64.
- Prabowo, D. S., Mujito, M., & Darmawan, D. 2024. Regulation of Criminal Acts of Narcotics Abuse in the Narcotics Law. *Bulletin of Science, Technology and Society*, 3(1), 46-51.
- Prasetyo, A. C., Saputra, R., & Wijaya, K. 2024. Procedural Justice and Public Understanding of Victim Restitution Rights. *Studi Ilmu Sosial Indonesia*, 4(2), 305-328.
- Purnomo, A. A., Negera, D. S., & Darmawan, D. (2025). Fair and Accountable Electronic Transactions: The Urgency of Consumer Protection, the Validity of Digital Contracts, and the Optimisation of Preventive and Repressive Dispute Resolution. *Studi Ilmu Sosial Indonesia*, 5(2), 43-64.
- Purwanto, D., Hardyansah, R., & Darmawan, D. 2025. Counterfeit Product Sales in Traditional Markets and Public Attitudes. *Studi Ilmu Sosial Indonesia*, 5(1), 139-166.
- Purwanto, I., Darmawan, D., Dirgantara, F., & Halizah, S. N. 2023. Implementation of Cosmetic Product Labeling Regulations for Consumer Protection and Fair Competition in the Marketplace. *Journal of Social Science Studies*, 3(1), 165-170.
- Putri, N. M. D. G., & Girinatha, D. G. W. 2024. Legal protection of personal data of indonesian citizens based on act number 27 of 2022. *Jurnal Notariil*, 9(2), 71-75. <https://doi.org/10.22225/jn.9.2.2024.71-75>
- Radjawane, L. E., & Mardikaningsih, R. 2022. Building Ethical and Fair Technology: Approaches to Responsible Technology Development and Application. *Journal of Social Science Studies*, 2(1), 189-194.
- Rahman, A., Darmawan, D., & Saputra, R. 2024. Analysis of Cross-border Payment Regulation and its Impact on Consumers in Indonesia. *Bulletin of Science, Technology and Society*, 3(2), 23-28.
- Ramle, N. L. B., & Mardikaningsih, R. 2022. Inclusivity in Technology-Based Services: Access and Skills Challenges. *Journal of Social Science Studies*, 2(2), 225-230.
- Rawi, M., N. H. Pakpahan, & P. Saktiawan. 2026. The Finality of Acquittal in Indonesian Criminal Procedure Law, *Studi Ilmu Sosial Indonesia*, 6(1), 1-24.
- Rezkiyanti, D. T., Wahyudi, W., Rezkiyanti, D. T., & Wahyudi, W. 2025. Legal Protection For Consumers In The Process Of Online Buying And Selling Transactions In The Marketplace. *Jurnal Ekonomi Kuntansi Manajemen Bisnis Dan Teknik Global*. 1(3), 264-272
- Rianto, R., Darmawan, D., & Negara, D. S. 2023. The Application of Restorative Justice in Resolving Speech Cases in the Digital Space: A Normative Analysis of the Electronic Information and Transactions Law and the Criminal Code. *Journal of Social Science Studies*, 3(1), 295-306.

- Rizaldy, B. M., Waskito, S., & Putra, A. R. 2023. Constructing Social Acceptance of Former Prisoners After Release through Citizenship Relations. *Studi Ilmu Sosial Indonesia*, 3(2), 309-332.
- Rojak, J. A., Khayru, R. K., & Darmawan, D. 2021. Citizens' Political Participation in Electoral Democracy and the Dynamics of Civil Society Movements. *Studi Ilmu Sosial Indonesia*, 1(1), 161-176.
- Ruohonen, J. 2023. Recent Trends in Cross-Border Data Access by Law Enforcement Agencies. *arXiv*. <https://doi.org/10.48550/arXiv.2302.09942>
- Rusianto, R., Hardyansah, R., & Darmawan, D. 2023. Application of the Elements of Money Laundering Crime in Indonesian Jurisprudence. *Bulletin of Science, Technology and Society*, 2(3), 44-50.
- Sahid, R. R., Hardyansah, R., Darmawan, D., Negara, D. S., & Khayru, R. K. 2023. Legal Perspective of Investment Risk Mitigation on Peer-to-peer Lending Platforms. *Journal of Social Science Studies*, 3(1), 177-184.
- Sajjapong, T., Darmawan, D., & Marsal, A. P. 2022. The Role of Social Stereotypes in Shaping Opportunities and Inequalities in Society: Their Impact on Education, Employment, and Intergroup Interactions. *Bulletin of Science, Technology and Society*, 1(1), 44-49.
- Saktiawan, P., Hardyansah, R., Darmawan, D., & Putra, A. R. 2021. Ethical Principles in Indonesian Legal Advocacy: Sustaining Justice in Adversarial Systems Through Professional Integrity. *Journal of Social Science Studies*, 1(2), 239-244.
- Samantaray, R. R., & Azeez, A. 2024. Data Privacy and Data Security in Electronic Records. *IGI Global*, 179-212. <https://doi.org/10.4018/979-8-3693-9591-2.ch007>
- Saputra, R., Prayitno, S., & Dirgantara, F. 2025. The Indonesian Criminal Justice System in Optimising the Recovery of State Assets: Structural Obstacles and the Urgency of Adopting Non-Conviction-Based Asset Forfeiture. *Studi Ilmu Sosial Indonesia*, 5(2), 23-42.
- Shulha, V., & Kaliuzhna, L. 2025. Electronic Evidence in Criminal Procedure: Methods for Its Detection, Investigation and Legal Consolidation. *Theory and Practice of Forensic Science and Criminalistics*. <https://doi.org/10.32353/khrife.3.2025.10>
- Sidabutar, A., Risdalina, R., & M, I. K. 2024. 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. *Enrichment*, 2(2), 60-65. <https://doi.org/10.55324/enrichment.v2i2.108>
- Sinambela, E. A. & D. Darmawan. 2022. Advantages and Disadvantages of Using Electronic Money as a Substitute for Cash, *Journal of Social Science Studies*, 2(2), 56-61.
- Sinambela, E. A., & Darmawan, D. 2022. Strengths and Weaknesses of Using Electronic Money as a Substitute for Cash. *Journal of Social Science Studies*, 2(2), 56-61.
- Sinambela, E. A., Nurmalasari, D., Darmawan, D., & Mardikaningsih, R. 2021. The Role of Business Capital, Level of Education, and Technology in Increasing Business Income. *Studi Ilmu Sosial Indonesia*, 1(1), 77-92.

- Suhartono, S., Sudjai, S., Darmawan, D., Rizky, M. C., & Saktiawan, P. 2024. The Effectiveness of Criminal Sanctions in Preventing Corruption: A Literature Review of the Indonesian Legal System. *Bulletin of Science, Technology and Society*, 3(3), 43-48.
- Sulani, S., Darmawan, D., Suwito, S., Mardikaningsih, R., & Gautama, E. C. 2025. Private Sales Deeds In Land Disputes: Weaknesses In Evidence And Registration Obstacles. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, 5(3), 4194-4218.
- Supriyanto, H., Salam, S., Muthmainna, W. N. A., Hasni, H., & Supardi, S. 2023. Criminal Asset Forfeiture In The Sense Of Extraordinary Confiscation. *Musamus Law Review*, 5(2). <https://doi.org/10.35724/mularev.v5i2.5425>
- Suryana, A., & Sakmaf, M. S. 2025. Can Electronic Evidence Constitute Sufficient Grounds for Criminal Liability? *Jurnal Ilmu Hukum Kyadiren*, 7(1), 587-601. <https://doi.org/10.46924/jihk.v7i1.323>
- Udjari, H., Hardyansah, R., Da Silva, E. B., & Cruz, C. da. 2022. Integrating Restorative Justice into Offender Rehabilitation Programs. *Journal of Social Science Studies*, 2(2), 201-206.
- Utama, S. P., Suwito, S., Waskito, S., & Khayru, R. K. 2024. Legal Protection of Juvenile Offenders Through Diversion, Development, and Social Reintegration in the Criminal Justice System. *Studi Ilmu Sosial Indonesia*, 4(2), 1-20.
- Vučković, B., & Vuckovic, V. 2025. Digital evidence in court proceedings: Between law and justice. *Pravni Život*, 370-379. <https://doi.org/10.5937/pdsc25370v>
- Wibisono, M. R., Rizky, M. C., & Sudjai. 2023. Norm Certainty and Enforcement Legitimacy in Local Public Order Regulation. *Studi Ilmu Sosial Indonesia*, 3(2), 223-246.
- Wibowo, A. S., Darmawan, D., Halizah, S. N., & Mardikaningsih, R. 2023. Optimizing the Principles of Healthy Business Competition and the Role of KPPU for a Fair Economy in the Digital Era. *Journal of Social Science Studies*, 3(1), 95-100.
- Wibowo, A. S., Darmawan, D., Negara, D. S., & Hardyansah, R. 2023. Analysis of Value Added Tax Application on Electronic Commerce Transaction in Digital Economy System in Indonesia. *Journal of Social Science Studies*, 3(2), 83-88.
- Wijaya, F. P., Safira, M. E., & Darmawan, D. 2022. Application of Restorative Justice in Criminal Case Settlement in Indonesia: A Literature Perspective. *Bulletin of Science, Technology and Society*, 1(3), 30-36.
- Wiyandarini, G., Hariani, M., & Mardikaningsih, R. 2021. Community-based Institutional Financing Model through Cooperatives for Micro and Small Enterprises. *Journal of Social Science Studies*, 1(1), 263-268.
- Yuristiawan, A., Darmawan, D., & Hardyansah, R. 2024. Digital Credit Regulations in Business Law and Financial Markets. *Journal of Social Science Studies*, 4(1), 371-380.
- Zulkarnain, A., Darmawan, D., & Hardyansah, R. 2024. Effectiveness of Law No. 5 of 1999 in Handling Cross-Border Business Competition. *SAPIENTIA ET VIRTUS*, 9(2), 461-475.