

INTERNATIONAL JOURNALOF LAW AND CONSTITUTION STUDY

Journal home page:https://jurnal.asrypersadaquality.com/index.php/ijlacos

ELECTRONIC EVIDENCE FROM THE PERSPECTIVE OF PROCEDURAL JUSTICE AND HUMAN RIGHTS

Naufal Rizky Fadhilah, M Yusuf Alamsyah Harahap, Livia Maylisandi, Tasya Afrianti Rambe

Islamic Criminal Law, Faculty of Sharia and Law, State Islamic University of North Sumatra

naufalfadhilah2019@gamil.com,yusufharahap59@gmail.com,maylisandilivia@gmail.com, tasyaafrianti24@gmail.com

ABSTRACT

The development of information technology has encouraged the use of electronic evidence as an important evidentiary tool in modern justice systems. Electronic evidence, such as digital documents, electronic messages, communication records, and transaction data, plays a role in helping to uncover legal facts and support more effective law enforcement processes. However, the use of electronic evidence also poses legal challenges, particularly related to fulfilling the principles of procedural justice and protecting human rights. Problems arise when the process of collecting, storing, or using electronic evidence is carried out without regard to applicable legal procedures, potentially violating the rights to privacy, communication confidentiality, and personal data protection. This study aims to analyze the position of electronic evidence from the perspective of procedural justice and human rights. The research method used is normative legal research with a statutory and conceptual approach through a literature review of various relevant legal sources. The results show that electronic evidence has important evidentiary value in the judicial process, but its use must comply with the principles of legality, authenticity, integrity, and accountability. In addition, the application of electronic evidence must continue to guarantee the protection of the basic rights of each individual to prevent abuse of authority in the law enforcement process. Therefore, a balance is needed between the interests of proof and the protection of human rights in order to realize a fair, transparent and just judicial process.

KEYWORDS

Electronic Evidence, Procedural Justice, Human Rights, Digital Evidence, Legal Protection..

Corresponding Author: Naufal Rizky Fadhilah

Article History	Submitted: March 16, 2026	Revision: March 18, 2026	Accepted: March 30, 2026	Published: July 30, 2026

https://doi.org/10.63736/ijlacos.v3i1

INTRODUCTION

The development of information and communication technology in the digital era has brought significant changes to people's lives, including in the legal and judicial systems. Various human activities previously carried out conventionally have now shifted to digital platforms, resulting in electronic traces that can be used as sources of information in law enforcement processes. The use of smartphones, social media, electronic mail (e-mail), instant messaging services, electronic transactions, and cloud-based data storage has created various forms of electronic data that have the potential to become evidence in the legal process. This condition shows that technological developments not only provide benefits to society but also present new challenges in the legal evidence system, which must be able to adapt to changing times (Brenner, 2010).

In modern legal systems, electronic evidence has become a crucial tool in uncovering various crimes. Electronic evidence is no longer limited to cybercrime, but is also used in corruption, money laundering, human trafficking, terrorism, narcotics, fraud, and other common crimes. Electronic evidence often has high probative value because it can record an event more objectively than witness testimony, which can be influenced by human subjectivity. Therefore, the use of electronic evidence has become an unavoidable necessity in law enforcement in the digital era (Casey, 2011).

In Indonesia, the recognition of electronic evidence as valid evidence has a legal basis through Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016. Article 5 paragraph (1) of the ITE Law emphasizes that electronic information and/or electronic documents and their printouts constitute valid legal evidence. This provision expands the evidentiary system previously regulated in Article 184 of the Criminal Procedure Code (KUHAP), which only recognized five forms of evidence, namely witness statements, expert statements, letters, clues, and statements from the accused. The presence of electronic evidence is a form of legal response to increasingly complex and dynamic technological developments (Makarim, 2020).

Despite its legal recognition, the use of electronic evidence in judicial practice still raises various legal issues. One of the main issues relates to the authenticity, integrity, and reliability of the electronic data submitted as evidence. Unlike conventional evidence, electronic data is characterized by its ease of modification, copying, transfer, or even deletion without leaving a clear trace.

Therefore, specific mechanisms and procedures are needed to ensure that electronic evidence submitted in court truly reflects the actual conditions and has not been manipulated during the collection or storage process (Casey, 2011).

Beyond technical issues, the use of electronic evidence is also closely related to the principle of procedural justice. Procedural justice is a concept that emphasizes that legal processes must be carried out based on fair, transparent, non-discriminatory procedures, and respect the rights of every individual involved in the judicial process. From this perspective, a decision is judged not only by its final outcome, but also by how the process was carried out. The use of electronic evidence obtained through unlawful means, such as unauthorized wiretapping, hacking of information systems, or forced data collection without a clear legal basis, has the potential to violate the principle of procedural justice and undermine the legitimacy of the judicial system itself (Tyler, 2006).

The principle of procedural fairness also requires equal opportunity for all parties to examine, test, and refute evidence presented in court. In the context of electronic evidence, this presents a particular challenge because not all parties possess sufficient technical skills to understand the characteristics of digital data. Therefore, the role of digital forensic experts is crucial in explaining the technical aspects of electronic evidence so that judges can objectively and proportionally assess the strength of the evidence. Without adequate testing mechanisms, electronic evidence has the potential to cause injustice and diminish the defendant's right to an effective defense (Murphy, 2007).

In addition to procedural justice, the use of electronic evidence is also closely linked to the protection of human rights. Various international human rights instruments, such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), guarantee every individual the right to privacy, freedom of expression, protection from arbitrary interference, and the right to a fair trial. The collection and use of electronic evidence often involve access to a person's personal data, potentially leading to privacy violations if conducted without a clear legal basis and effective oversight mechanisms (United Nations Human Rights Committee, 1988).

The right to privacy is one of the fundamental rights most vulnerable to the use of electronic evidence. In law enforcement practice, authorities frequently conduct communications interception, electronic device inspections, digital data collection, or online activity monitoring as part of the investigative process. While these actions may be justified for law enforcement purposes, their implementation must adhere to the principles of legality, proportionality, and accountability to prevent them from becoming human rights violations. In other words, the state's interest in eradicating crime must be balanced with its obligation to protect individual rights from abuse of power (Solove, 2021).

Technological developments have also sparked debate over the limits of state authority in obtaining electronic evidence. On the one hand, the state has an obligation to maintain public order and security through effective law enforcement. However, on the other hand, excessive use of surveillance technology can lead to mass surveillance practices that threaten civil liberties and citizens' privacy rights. Therefore, a balance is needed between the interests of law enforcement and the protection of human rights to ensure that the judicial process continues to operate in accordance with the principles of a democratic state governed by the rule of law (Roach, 2021).

In Indonesian judicial practice, various cases demonstrate that electronic evidence is often a determining factor in proving a case. However, many cases also give rise to controversy regarding the legality of obtaining electronic evidence, the authority of law enforcement officials, and the protection of the rights of suspects and defendants. This situation indicates that the regulation of electronic evidence is not only related to the technical aspects of proof, but also concerns issues of ethics, justice, and respect for human rights. Therefore, a comprehensive study of electronic evidence is necessary to provide a complete understanding of its legal implications in the modern justice system (Kerr, 2005).

Based on this description, this research is crucial for analyzing the position of electronic evidence in the Indonesian legal system from the perspective of procedural justice and human rights. It also aims to assess the extent to which the mechanisms for using electronic evidence comply with the principle of due process of law and guarantee the protection of the fundamental rights of every individual in the judicial process. Therefore, the research findings are expected to contribute academically to the development of evidentiary law in Indonesia and serve as evaluation material for formulating legal policies that are more adaptive to the development of digital

technology without neglecting the principles of justice and respect for human rights.

RESEARCH METHODS

This research uses a normative legal research method (normative juridical) with a descriptive-analytical nature. Normative legal research is conducted by examining library materials or secondary data consisting of laws and regulations, legal doctrine, court decisions, and various literature relevant to the research object. This method was chosen because the research focuses on analyzing the position of electronic evidence in the Indonesian legal evidence system and its implications for the principles of procedural justice and human rights protection.

The approaches used in this research include the statute approach, the conceptual approach, and the case approach. The statutory approach is carried out by reviewing various regulations related to electronic evidence, such as the 1945 Constitution of the Republic of Indonesia, the Criminal Procedure Code (KUHAP), Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016, Law Number 39 of 1999 concerning Human Rights, and other relevant laws and regulations. The conceptual approach is used to analyze the theory of procedural justice, due process of law, and the concept of human rights protection in the evidentiary process. Meanwhile, the case approach is carried out by reviewing court decisions related to the use of electronic evidence in the judicial process.

The legal sources used in this study consist of primary legal materials, secondary legal materials, and tertiary legal materials. Primary legal materials include laws and regulations, court decisions, and international legal instruments related to human rights. Secondary legal materials include law books, scientific journals, previous research results, academic articles, and expert opinions discussing electronic evidence, criminal procedure law, procedural justice, and human rights. Tertiary legal materials include legal dictionaries, legal encyclopedias, and other reference sources supporting the research.

The legal material collection technique was conducted through library research by inventorying, identifying, and reviewing various legal sources relevant to the research problem. Next, the collected legal material was analyzed using qualitative analysis methods, namely by interpreting, connecting, and evaluating various legal norms and theories related to the use of electronic evidence from the perspective of procedural

justice and human rights. The results of the analysis were then systematically compiled to obtain conclusions regarding the suitability of the regulation and application of electronic evidence with the principles of procedural justice and human rights protection in the Indonesian legal system.

RESULTS AND DISCUSSION OF

RESULTS

Based on research into various laws and regulations, legal literature, and court decisions related to the use of electronic evidence, it was found that the Indonesian legal system has provided strong recognition of electronic information and/or electronic documents as valid evidence in judicial proceedings. This recognition is regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016, which expands the evidentiary system beyond the provisions of Article 184 of the Criminal Procedure Code (KUHAP). With this regulation, electronic evidence has equal legal standing with other evidence as long as it meets the validity requirements stipulated by law (Makarim, 2020).

Advances in information technology have led to the increased use of electronic evidence in various criminal justice processes. Electronic evidence is used not only in cybercrime cases, but also in corruption, money laundering, narcotics, terrorism, and various other crimes. Electronic data in the form of text messages, emails, digital recordings, electronic transactions, and communication data are often used to strengthen evidence in court. This situation indicates that electronic evidence has become a vital part of the modern evidentiary system, inseparable from the development of digital technology (Fernando et al., 2024).

Research results show that the validity of electronic evidence is highly dependent on the authentication, integrity, and reliability of the data used as evidence. Unlike conventional evidence, electronic data is characterized by its ease of copying, transferring, modifying, and even deleting without leaving any easily detectable traces. Therefore, the application of digital forensics is a crucial tool in ensuring that electronic evidence presented in court is authentic and unchanged since it was first obtained by law enforcement (Casey, 2011).

This study also found that in judicial practice, judges not only assess the existence of electronic evidence but also consider the process by which it was obtained. Electronic evidence obtained through unlawful procedures has the potential to lose its evidentiary value. Therefore, the application of the principle of due process of law is a

crucial aspect in the use of electronic evidence. This principle requires that every process of collecting, storing, and presenting evidence be carried out in accordance with applicable law to ensure justice for all parties involved in the judicial process (Tyler, 2006).

From a procedural justice perspective, research shows that the use of electronic evidence should provide equal opportunity for all parties to examine, test, and refute the evidence presented in court. The defendant's right to know the source of evidence, the method of obtaining evidence, and the process of examining electronic evidence is an essential part of the principle of fair trial. Therefore, transparency in the management of electronic evidence is a key requirement for achieving procedural justice in the criminal justice system (Murphy, 2007).

In addition to concerns about procedural fairness, the use of electronic evidence is also closely linked to the protection of human rights. Research has found that electronic data collection often involves access to a person's personal information, including electronic communications, location data, social media activity, and other digital documents. Under certain circumstances, such actions can pose a risk of violating the right to privacy if not conducted in accordance with clear and proportionate legal provisions. Therefore, protecting the right to privacy must be a primary consideration in the use of electronic evidence as evidence (United Nations Human Rights Committee, 1988).

Furthermore, research shows that the development of digital surveillance technology has created new challenges in human rights protection. The state has an obligation to enforce the law and maintain public security, but this authority must not be used excessively to the point of compromising citizens' fundamental rights. The principles of legality, proportionality, and accountability must be applied in every act of collecting electronic evidence to prevent abuse of authority by law enforcement officials (Solove, 2021).

The research also shows that regulations regarding electronic evidence in Indonesia still require strengthening, particularly regarding standards for obtaining, examining, and evaluating electronic evidence in judicial proceedings. Although the ITE Law provides a legal basis for the use of electronic evidence, there is still a need to clarify the mechanisms for its implementation to create legal certainty and optimal human rights protection. Strengthening these regulations is crucial given the rapid

development of technology and the continued emergence of new forms of digital evidence that are not yet fully accommodated by existing regulations (Roach, 2021).

Overall, the research findings indicate that electronic evidence plays a crucial role in supporting the effectiveness of modern evidentiary systems. However, its use must always adhere to the principles of procedural fairness and human rights protection to ensure that law enforcement objectives are achieved in a balanced manner. In other words, the successful use of electronic evidence is determined not only by the sophistication of the technology used, but also by the extent to which the process respects the fundamental rights of every individual in a democratic state governed by the rule of law (Kerr, 2005).

DISCUSSION

The Position of Electronic Evidence in the Indonesian Legal Evidence System

The development of information and communication technology has transformed the pattern of social interaction from conventional to digital. This transformation has resulted in various forms of electronic information that can be used as evidence in judicial proceedings. In the context of Indonesian law, the recognition of electronic evidence as valid evidence represents the state's response to the increasingly rapid technological developments. Prior to the enactment of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), the evidentiary system in Indonesian criminal procedure law only recognized evidence as regulated in Article 184 of the Criminal Procedure Code, namely witness testimony, expert testimony, letters, instructions, and the defendant's testimony. The introduction of the ITE Law broadened the evidentiary system by recognizing electronic information and electronic documents as valid legal evidence (Makarim, 2020).

This recognition demonstrates that Indonesian law has adapted to the development of the digital society. Electronic information can include recorded conversations, emails, text messages, CCTV footage, electronic transactions, social media data, and various other forms of digital data relevant to a legal case. In practice, electronic evidence is often the primary source of evidence capable of explaining the relationship between the perpetrator, the criminal incident, and the resulting legal consequences (Kerr, 2005).

However, the existence of electronic evidence cannot be separated from the issue of data authenticity and validity. Unlike conventional evidence that can be directly

observed, electronic evidence is characterized by its ease of copying, modification, or even deletion without leaving any visible physical changes. Therefore, the validity of electronic evidence must be tested through a rigorous authentication process to ensure that the data truly originates from a legitimate source and has not been altered since it was first obtained (Casey, 2011).

From the perspective of evidentiary law, the recognition of electronic evidence not only aims to increase the effectiveness of law enforcement but also to provide legal certainty in the face of developments in digital technology. Therefore, the position of electronic evidence in the Indonesian legal system is part of the modernization of procedural law, which aims to create an evidentiary system that is more adaptive to current developments (Fernando et al., 2024).

1. Analysis of Procedural Fairness in the Use of Electronic Evidence

The concept of procedural justice emphasizes that a legal process must be carried out based on fair, transparent procedures that respect the rights of all individuals involved. According to Tyler (2006), the public tends to accept legal decisions if the process used to produce them is perceived as fair. Therefore, in the use of electronic evidence, the primary focus lies not only on the final outcome of the evidence, but also on how the evidence is obtained and used.

The application of procedural justice requires law enforcement officials to obtain electronic evidence through legitimate procedures. Wiretapping, digital surveillance, electronic data collection, and examination of digital devices must be conducted based on clear legal authority. Evidence obtained through unlawful means has the potential to violate the principle of due process of law and undermine the legitimacy of the judicial process (Tyler, 2006).

In judicial practice, problems often arise when electronic evidence is obtained without the consent of the data owner or without adequate oversight mechanisms. This situation raises questions about the limits of law enforcement's authority to obtain digital data. Therefore, any act of collecting electronic evidence must comply with the principle of legality, meaning that it must be carried out in accordance with applicable legal provisions and not exceed the authority granted by law (Roach, 2021).

Beyond legality, the principle of transparency is also an essential component of procedural fairness. Defendants must be given the opportunity to learn about the sources of evidence, data collection methods, and the digital examination process

conducted by investigators. This right is part of the principle of equality of arms, which is the balance of rights between the public prosecutor and the accused in the judicial process (Murphy, 2007).

Thus, the use of electronic evidence that meets the principles of procedural justice will increase public trust in the justice system and prevent abuse of authority by law enforcement officers.

2. Electronic Evidence and Human Rights Protection

The use of electronic evidence is closely linked to the protection of human rights, particularly the right to privacy, the right to protection of personal data, and the right to a fair trial. In the digital age, almost every individual activity leaves an electronic footprint stored in various devices and information systems. Consequently, the process of collecting electronic evidence often involves access to an individual's personal information (Solove, 2021).

The right to privacy is a fundamental right recognized in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). These provisions emphasize that no one shall be subjected to arbitrary interference with his or her private life, family, home, or correspondence (United Nations Human Rights Committee, 1988).

In the context of the use of electronic evidence, protecting the right to privacy is a crucial issue. The collection of communication data, access to social media, and interception of electronic conversations must be carried out proportionally and based on legitimate grounds. If carried out without a clear legal basis, such actions can be categorized as human rights violations (Solove, 2021).

In addition to the right to privacy, the use of electronic evidence also relates to the right to a fair trial. Every individual has the right to know the evidence used against them and to have the opportunity to refute or challenge the validity of that evidence. This right is part of the principle of due process of law, a key pillar of a democratic state based on the rule of law (Murphy, 2007).

Therefore, human rights protection in the use of electronic evidence must be a primary consideration in every law enforcement process. The state has an obligation to balance the interests of eradicating crime with the protection of citizens' fundamental rights.

3. The Role of Digital Forensics in Ensuring the Validity of Electronic Evidence

Digital forensics is a branch of forensic science that identifies, obtains, examines,

analyzes, and presents electronic data as evidence in court. In the context of evidence, digital forensics plays a crucial role because the characteristics of electronic evidence differ from those of conventional evidence (Casey, 2011).

One of the primary functions of digital forensics is to maintain data integrity through the implementation of the chain of custody. The chain of custody of evidence is necessary to ensure that electronic data remains unchanged from the time it is first discovered until it is presented in court. If the chain of custody cannot be proven, the validity of electronic evidence can be questioned (Fernando et al., 2024).

Furthermore, digital forensics also functions to identify potential data manipulation. Using scientific methods, digital forensic experts can determine whether an electronic document has been modified, deleted, or falsified. This ability is crucial for maintaining the objectivity and accuracy of the evidence process (Casey, 2011).

Increasingly complex technological developments demand increased capacity among law enforcement officials in the field of digital forensics. Without the support of competent human resources and adequate technology, the use of electronic evidence has the potential to lead to errors in the evidentiary process, ultimately harming those seeking justice.

According to the author, the existence of electronic evidence is an unavoidable necessity in the modern justice system. The development of digital technology has transformed the way humans communicate and interact, resulting in most societal activities now leaving electronic traces that can be used as evidence. Therefore, recognizing electronic evidence is an appropriate step in reforming Indonesian criminal procedure law.

However, the effective use of electronic evidence must be balanced with protection of the principles of procedural justice and human rights. Law enforcement that focuses solely on the effectiveness of evidence without regard for individual rights has the potential to give rise to abuse of authority. Conversely, overly rigid human rights protection without considering the needs of law enforcement can also hamper the process of eradicating crime.

Thus, a balance between law enforcement interests, procedural fairness, and human rights protection must be the primary basis for the use of electronic evidence. Strengthening regulations, increasing digital forensic capacity, and effective oversight of the electronic evidence acquisition process are necessary steps to achieve a just,

transparent, and human rights-oriented justice system.

CONCLUSION

The development of information and communication technology has brought significant changes to the legal evidence system in Indonesia. The presence of electronic evidence as valid evidence demonstrates that Indonesian law has strived to adapt to the increasingly complex developments in the digital society. Through Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016, electronic information and/or electronic documents and their printouts have been recognized as legally binding evidence in judicial proceedings. This recognition provides a strong legal basis for law enforcement officials in utilizing digital technology to uncover various crimes that are increasingly widespread in the modern era. Electronic evidence is not only used in cybercrime cases, but has also become an important part of proving cases of corruption, money laundering, narcotics, terrorism, fraud, and various other crimes.

Despite its crucial role in supporting effective law enforcement, the use of electronic evidence cannot be separated from the principle of procedural justice. This research shows that the validity of electronic evidence is determined not only by its content or information, but also by the process of obtaining, storing, examining, and presenting it to the court. Electronic evidence obtained through unlawful means has the potential to violate the principle of due process of law and undermine the legitimacy of the judicial process. Therefore, every stage of the use of electronic evidence must be conducted transparently, accountably, and in accordance with applicable legal provisions. Procedural justice is a crucial aspect because it ensures that each party has an equal opportunity to learn about, examine, and refute the evidence presented in court, thus creating a fair and non-discriminatory judicial process.

From a human rights perspective, the use of electronic evidence is closely linked to the protection of the right to privacy, personal data protection, and the right to a fair trial. In practice, the collection of electronic evidence often involves access to personal data, digital communications, and various confidential information. Therefore, the use of electronic evidence must be implemented based on the principles of legality, proportionality, and accountability to avoid violating citizens' fundamental rights. The state has an obligation to ensure that law enforcement efforts are not carried out in a manner that compromises human rights. Striking a balance between the interests of law enforcement and the protection of individual rights is a key requirement for

realizing a democratic and just justice system.

This study also found that digital forensics plays a crucial role in ensuring the authenticity, integrity, and reliability of electronic evidence. Given the easily copied, modified, transferred, or deleted nature of digital data, scientific methods are needed to ensure that electronic evidence presented in court is truly authentic and legally admissible. Digital forensics not only assists law enforcement in uncovering legal facts but also serves as an instrument to protect the rights of the parties in the judicial process. With professional and objective digital forensic examinations, the quality of evidence can be improved while minimizing the risk of errors in law enforcement.

Based on the overall research findings, it can be emphasized that electronic evidence is a crucial instrument in the modern justice system and plays a significant role in supporting the effectiveness of evidence in the digital era. However, its use must always be placed within the framework of a state based on the rule of law that upholds the principles of procedural justice and respect for human rights. Therefore, it is necessary to strengthen more comprehensive regulations, increase the capacity of law enforcement officials in the fields of technology and digital forensics, and implement more effective oversight of the process of obtaining and using electronic evidence. With these steps, the use of electronic evidence will not only support the success of law enforcement but also guarantee the protection of citizens' rights and realize a fair, transparent, and substantive justice-oriented justice system.

REFERENCE

Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press.

Fernando, D., Heniarti, DD, & Zakaria, CAF (2025). Transforming electronic evidence using digital forensics in the reform of criminal procedural law. *Journal Justiciabelen (JJ), 5(1), 1–*15.https://jurnal.unsur.ac.id/index.php/JJ/article/view/5506

Hamzah, A. (2019). *Indonesian Criminal Procedure Law*. Sinar Grafika.

Harahap, MY (2016). *Discussion of issues and application of the Criminal Procedure* Code: Examination of court hearings, appeals, cassation, and judicial review. Sinar Grafika.

Kerr, O. S. (2005). Digital evidence and the new criminal procedure. Columbia Law

Review, 105(1), 279–318.

Makarim, E. (2020). *Introduction to telematics law: A compilation of studies*. Rajawali Pers.

Murphy, P. (2007). *Murphy on Evidence (10th ed*.). Oxford University Press.

Nelson, R. (2022). A legal analysis of the use of electronic information *(digital evidence) as valid evidence in criminal procedure law*. Lex Privatum, 10(5).https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/42831

Rahardjo, A. (2014). *Telematics and information technology law*. Citra Aditya Bakti.

Roach, K. (2021). *Criminal law and procedure in the digital age*. Cambridge University Press.

Solove, DJ (2021). *Understanding privacy (2nd ed.).* Harvard University Press.

Sumarahati, AS, & Irawan, A. (2024). A legal analysis of human rights protection in electronic law enforcement (E-Law Enforcement). *Indonesian Journal of Islamic Jurisprudence*, Economic and Legal Theory.https://shariajournal.com/index.php/IJIJEL/article/view/563

Tyler, T. R. (2006). Why people obey the law (2nd ed.). Princeton University Press.

United Nations. (1948). Universal Declaration of Human Rights.https://www.un.org/en/about-us/universal-declaration-of-human-rights

United Nations. (1966). International Covenant on Civil and Political Rights (ICCPR).https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

United Nations Human Rights Committee. (1988). General Comment No. 16: Article 17 (Right to Privacy).https://www.refworld.org/docid/453883f922.html

Wachjoe, R. (2016). The position of electronic evidence in the Indonesian criminal law evidence system. *Journal of Law and Justice*, 5(1), 89–104.https://www.jurnalhukumdanperadilan.org

Republic of Indonesia. (1945). *The 1945 Constitution of the Republic of Indonesia*.

Republic of Indonesia. (1981). *Law Number 8 of 1981 concerning Criminal Procedure* Law.

Republic of Indonesia. (1999). Law Number 39 of 1999 concerning Human Rights.

Republic of Indonesia. (2008). *Law Number 11 of 2008 concerning Electronic* Information and Transactions.

Republic of Indonesia. (2016). *Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions*.