Evaluation of Electronic Evidence in Criminal Justice in the Era of Advanced Artificial Intelligence Technology

Benny Sumardiana[1] ✉, Pujiyono[2], Irma Cahyaningtyas[3], Cahya Wulandari[4]

[1] Faculty of Law, Universitas Negeri Semarang, Semarang, Indonesia.
https://orcid.org/0000-0001-5087-6973
[2] Faculty of Law, Universitas Bengkulu, Bengkulu, Indonesia.
https://orcid.org/0000-0001-8244-8092
[3] Faculty of Law, Universitas Diponegoro, Semarang, Indonesia.
https://orcid.org/0000-0003-2911-1268
[4] Faculty of Law, Universitas Negeri Semarang, Semarang, Indonesia.
https://orcid.org/0000-0003-1034-7916

✉ Corresponding Email: Benny.sumardiana@mail.unnes.ac.id

Abstract

Law enforcement is one of the many facets of society that have seen substantial changes as a result of the quick growth of digital technology, especially artificial intelligence (AI). The purpose of this study is to assess how electronic evidence is used in Indonesia's criminal justice system, pinpoint the difficulties encountered, and offer suggestions for enhancing the efficiency and equity of electronic evidence in the age of artificial intelligence. In line with the technological elements included in digital and criminal investigation research methodologies, this qualitative study aids in the creation of a theoretical framework for the use of electronic evidence in the setting of artificial intelligence. The results show that Indonesian law is now able to meet the needs of the digital age with its adaptation to technological advancements. Finding material truth in court proceedings is made possible by electronic evidence, which is legally acknowledged as a legitimate tool in criminal justice. To successfully address these issues

and optimize the use of AI in the legal system, it is imperative to develop a strong ethical framework, improve law enforcement capacities, and update rules on a regular basis.

Keywords

Electronic Evidence; Artificial Intelligence; Criminal Justice.

Introduction

"*In criminalibus probationes bedent esse luce clariores*", in criminal matters, evidence must be clearer than light. This adage illustrates the importance of the evidentiary process in criminal justice, which must be carried out very brightly and clearly. This expression emphasizes how crucial evidence in criminal justice is, which must be carried out transparently and without doubt. In an effort to create a civilized society, dignified and humane criminal justice practices are a must. This must be realized through a fair legal process, including in the process of evidence. After all, the imposition of criminal punishment is closely related to the most fundamental human rights, namely the right to life and freedom. Therefore, the process must be conducted carefully and accurately, to represent the absolute truth as much as possible.

Evidence is a provision that regulates legal evidence according to the law, which can be used by the judge to prove the defendant's guilt in accordance with the law and the judge's belief. Therefore, in a trial, the judge must not act arbitrarily or arbitrarily in proving the defendant's guilt.[1] Evidence is an important aspect of the criminal justice process, where this provision regulates the types of evidence recognized by law and which can be used by the judge to confirm or reject the allegations made against the defendant. Valid evidence, such as witness testimonies,

---

[1] Indra Janli Manope, "Kekuatan Alat Bukti Surat Elektronik Dalam Pemeriksaan Perkara Pidana," *Lex Crimen* Vol. VI No, no. Vol. VI/No. 2/Mar-Apr/2017 (2017): 107–13, https://ejournal.unsrat.ac.id/index.php/lexcrimen/article/view/15350/14898.

documents, and electronic evidence, must meet established legal standards in order to be considered in reaching a fair verdict. Judges, in carrying out their duties, are obliged to adhere to these evidentiary rules and use the available evidence carefully, based on the applicable laws and their personal beliefs formed from the entire trial process. Evidence has a very important role, so that in the process of examining a criminal case, all items used to commit a criminal offense or related to the criminal offense can be confiscated and used as evidence.

In the midst of the rapid development of digital technology, especially in artificial intelligence (AI), has brought significant changes in various aspects of life, including in law enforcement. In the context of criminal justice, the use of electronic evidence has become an increasingly relevant and important instrument, considering that conventional evidence is often unable to represent the dynamics of modern crimes involving sophisticated technology. the use of electronic evidence in criminal justice must be in line with the principles of justice, truth, and the protection of human rights. in the emergence of electronic evidence in the midst of this technological development will raise a lot of questions ranging from the extent to which technology can be relied upon in representing the truth? Is the use of electronic evidence exposed to AI technological manipulation still able to maintain substantive justice?

Electronic evidence can be portrayed as a two-eyed sword for law enforcement. On the one hand, these evidence tools can greatly ease law enforcement in finding the necessary evidence, meet the minimum of evidence, and be a strong basis in the proofing process in court. However, on the other hand, the use of electronic evidence tools often requires more in-depth verification and evidence to ensure that the evidence is truly valid and admissible before the court.[2] Electronic evidence is not only regulated in the Act that specifically regulates criminal acts, but also exists in other

---

[2]   Nurlaila Isima, "KEDUDUKAN ALAT BUKTI ELEKTRONIK DALAM PEMBUKTIAN PERKARA PIDANA" 5, no. 1 (2022): 179–89.

laws that are not specifically related to crime. Recognition of electronic evidence first appeared in the Act governing corporate documents. In this Act, electronic evidence is regarded as part of a corporate document and is treated as a documentary evidence. This recognition was then followed by various other legal regulations.

The ongoing digital transformation of society, the growth of cybercrime, therefore, the growing importance of proving the digital footprint of crimes, the de-facto mass use of electronic evidence in the practice of law enforcement agencies - all this is fraught with the problem of the absence of the notion of "electronic evidence" in criminal procedure law.[3] Such broad limitations on the use of electronic evidence can lead to problems at the level of its application in the handling of criminal cases. This challenge is especially felt by judges, who have the duty to adjudicate and base their decisions on the evidence available through the evidentiary process. One of the most crucial moments for a judge is when he or she must determine whether or not certain electronic evidence is admissible as valid evidence.[4]

In the United Arab Emirates (UAE), IT infrastructure has experienced enormous growth and the country is expected to become a leading tech giant by 2025.[5] In 2019, the revenue of IT companies based in the UAE, especially in Dubai is expected to reach around $6 billion, which is a growth of 12.5% compared to 2018. These IT companies in the United Arab Emirates need specialized support from digital forensics & audit service providers, which have also been growing rapidly in both

---

[3] A. A. Dmitrieva and P. S. Pastukhov, "Concept of Electronic Evidence in Criminal Legal Procedure," *Journal of Digital Technologies and Law* 1, no. 1 (2023): 270–95, https://doi.org/10.21202/jdtl.2023.11.

[4] Made Hartono, Sugi and Rai Yuliartini, Ni, Putu, "PENGGUNAAN BUKTI ELEKTRONIK DALAM PERADILAN PIDANA," *Nature Microbiology* 3, no. 1 (2020): 641, http://dx.doi.org/10.1038/s41421-020-0164-0%0Ahttps://doi.org/10.1016/j.solener.2019.02.027%0Ahttps://www.golder.com/insights/block-caving-a-viable-alternative/%0A???%0Ahttp://dx.doi.org/10.1038/s41467-020-15507-2%0Ahttp://dx.doi.org/10.1038/s41587-020-05.

[5] Dmitrieva and Pastukhov, "Concept of Electronic Evidence in Criminal Legal Procedure."

the public and private sectors. For example, Eshield IT Services is a Dubai-based cybersecurity company that is a leading provider of cybersecurity solutions. The company assists clients in implementing robust security measures to protect their businesses and organizations from cyber-attacks. EXEO is another multi-faceted cloud and cybersecurity provider agency, which helps its clients to identify risks, and protect and monitor their assets through business process automation and intelligent services. The practice of digital investigations is also governed by a well-defined legal framework, where the UAE police play a vital role in regulating and overseeing this complex process.[6] It is ensured that forensic and other services are designed to provide end-to-end capabilities and complete forensic and security solutions, for businesses. The UAE government ensures that these forensic services form a framework that is distinguished by its unwavering commitment to maintaining a strong legal foundation, maintaining data confidentiality, upholding professional ethical standards, and rigorously verifying the integrity of evidence. As a result, the UAE government facilitates the effective implementation of digital investigation procedures in this jurisdiction.[7]

Indonesia's criminal justice system is now faced with an urgent need to adapt to these technological developments. Law enforcement officials and legal practitioners need to understand the complexities of electronic evidence influenced by AI, and develop the necessary skills and tools to ensure the validity and reliability of such evidence. In the face of this situation, judges should have clear guidelines and procedures for assessing and qualifying electronic evidence. These guidelines are important so that judges can ensure that electronic evidence meets legal standards and is reliable in judicial proceedings. In addition, there need to be parameters used as a measure in selecting and evaluating electronic evidence so that judges can properly determine whether the evidence should be used as

---

[6] Fares Dahabreh, "The Continued Usage of Artificial Intelligence in the United Arab Emirates Public Sector Organisations: An Extended Information System Success Model," 2023, 1–287.

[7] Dahabreh.

valid evidence in the criminal justice process, especially in the context of rapidly developing AI technology. This study aims to evaluate how electronic evidence is used in Indonesia's criminal justice system, identify challenges faced, and provide recommendations to improve the effectiveness and fairness of the use of electronic evidence amidst the onslaught of AI technology.

Problem formula

1. What is the procedure for declaring the validity of electronic evidence in Indonesian trials based on Law Number 11 of 2008 concerning Electronic Information and Transactions in line with technological developments?
2. How is the use of Artificial Intelligence (AI) technology in criminal justice in Indonesia and how to deal with the challenges and advantages of using electronic evidence in the era of Artificial Intelligence (AI) technology sophistication?
3. How can the evaluation of the strength of electronic evidence in proving criminal offenses in Indonesia be carried out effectively and efficiently in the AI era?

Method

This research utilizes a qualitative research methodology to investigate the use of electronic evidence in criminal justice amidst the onslaught of artificial intelligence technology. This qualitative research effort is dedicated to the development of a theoretical framework for the application of e-evidence in the midst of AI, in line with the technological aspects inherent in digital and criminal investigation research methodologies. Therefore, the research strategy used in this study includes qualitative research, descriptive analysis, and analytical research, in an effort to obtain data, this study adopts normative juridical research methods and scientific research methods, both of which are well-

established techniques in the domain of legal studies. Data collection utilized primary and secondary data sources.

Data was collected by gathering primary legal materials, secondary legal materials, and non-legal materials through library research or website searches. This information was then inventoried to verify its veracity, after which it was grouped and analyzed using both approaches to obtain a thorough understanding and synchronization of all existing legal materials. Once the data was collected, it was analyzed using the descriptive method of analysis. This method focuses on the formulation of the problem at hand by collecting and reviewing available sources of legal material. The analysis is conducted in depth through a literature study by describing and sorting out each issue to ensure conformity with the formulation of the problem set.

Result and Discussion

A. Procedures for Verifying The Validity of Electronic Evidence

The limitations of evidence regulated in the Criminal Procedure Code, along with the times, are no longer able to fully accommodate the realities that occur in today's society. The disclosure of material truth in criminal cases will not achieve optimal results if it only relies on the five types of evidence that have been determined.[8] Electronic evidence itself includes digital data such as emails, audio and video recordings, as well as data obtained from computer devices and mobile phones, has become an important tool in law enforcement and judicial processes. This model of instrument is not covered by evidence as stipulated in Article 184 of KUHAP. Law No. 11/2008 on Electronic Information and Transactions (ITE Law) has provided an alternative in the use of electronic evidence to overcome the limitations in KUHAP. In cases of criminal offenses related to electronic information and transactions, the ITE Law expands the scope of evidence that can be used. Not only limited to traditional evidence as stipulated in the Criminal Procedure Code, the ITE Law also recognizes

---

[8]　Manope, "Kekuatan Alat Bukti Surat Elektronik Dalam Pemeriksaan Perkara Pidana."

electronic information, electronic documents, and their printouts as valid evidence in the eyes of the law.

Electronic Documents are types of electronic information that are produced, processed, scanned, scanned, transmitted, or stored in any format, including digital, analog, optical, electromagnetic, and so on. This document can be viewed, printed, and/or edited using a computer or electronic system. It contains various types of data, such as text, images, graphics, photographs, videos, audio files, symbols, letters, signs, and numbers. It can also be interpreted by people who are capable of understanding it. On the other hand, information, as defined in Article 1 of the ITE Law, is one or more complete sets of electronic data but does not include text, images, graphics, text data interchange (EDI), electronic mail (email), telegram, telek, telescope, and other similar formats. In addition, this data includes symbols, letters, signs, numbers, access codes, and other information that has been completed and is understandable to a person with the necessary knowledge to understand it. As a result, electronic signatures fall into the category of electronic documents or electronic information, designating them as secure and useful tools for document preparation, particularly in the field of electronic and information transactions. These developments show that Indonesian law has caught up with technological advances and is now capable of meeting the needs of the digital age.

The process of disclosing evidence in a criminal case is essentially an attempt to discover and disclose the material truth in relation to crimes and criminals committed by a person, so that the person can be punished. This procedure is subject to procedural laws that set out certain limitations, in particular regarding the type of evidence that can be used and the assessment of that evidence. Neither the Attorney General nor the accused, through their assistant lawyers, have complete freedom to propose evidence as they see fit. The role of the judge in assessing and weighing the

strength of the evidence is therefore important, with such assessment having to be based on evidence explicitly provided for by law.[9]

Proving whether the defendant actually committed the act charged is the most important aspect of criminal procedure law. Therefore, criminal procedure law focuses on the search for material truth. There are six main points that become benchmarks in the theory of evidence, which can be described as follows:[10]

1. Basis of Proof: Considerations used by the court to determine the true facts of a case (bewijsgronden). This basis of proof is the main footing in deciding whether a criminal event actually occurred based on the available evidence.

2. Tools of Evidence: Instruments or means used by the judge to build a picture of the criminal event that has occurred (bewijsmiddelen). These include various forms of evidence, such as testimonies, documents, and physical evidence, which assist in reconstructing past events.

3. Methods of Presenting Evidence: Describes the procedure or method used to present evidence to the judge at trial (bewijsvoering). This process includes the preparation and presentation of evidence in a legally acceptable manner and assists the judge in evaluating the veracity of the charges.

4. Strength of Proof: An assessment of the extent to which each piece of evidence has power in the course of proving a charge (bewijskracht). It determines how convincing the evidence is in proving or disproving the charges.

5. Mandatory Proof: The legal obligation to prove the truth of the charges before the court (bewijslast). The law stipulates that the charging party must be able to prove its allegations with sufficient evidence to support the charges.

---

[9]   Hartono, Sugi and Yuliartini, Ni, Putu, "PENGGUNAAN BUKTI ELEKTRONIK DALAM PERADILAN PIDANA."

[10] Isima, "KEDUDUKAN ALAT BUKTI ELEKTRONIK DALAM PEMBUKTIAN PERKARA PIDANA."

6. Minimum Evidence: The minimum amount or type of evidence required in evidence to ensure that judges are bound by certain standards in deciding cases (bewijsminimum). This minimum evidence serves as a lower limit that must be met for a charge to be considered proven.

The formal requirement for electronic evidence is that the evidence must not be in the form of documents or letters which according to the law must be in written form. If a party submits an electronic document in written form, the judge is obliged to reject it until the party concerned can present authentic letter evidence. In its development, Constitutional Court Decision No. 20/PUU-XIV/2016 states that electronic evidence can only be used for law enforcement purposes at the request of the police, prosecutors, and/or other law enforcement authorities regulated by applicable regulations. In order for electronic evidence to be used in legal proceedings, material and formal requirements must be met cumulatively.[11]

Electronic evidence that can be considered in court must not only fulfill the existing requirements, namely material and formal, but must also comply with the legal theory of evidence. This theory states that in order for a piece of evidence to be accepted in court, it must fulfill several conditions, namely being allowed by law as evidence; having *reliability* or trustworthiness; *necessity* or indeed needed to prove a fact; and *relevance* or relevant to the facts to be proven.[12]

In the ITE Law, there are provisions regarding the validity of electronic evidence that can be accepted as evidence, as stipulated in Article 6. These conditions include: accessible, displayable, guaranteed integrity,

---

[11] Eko Surya Prasetyo, Y.A. Triana Ohoiwutun, and Halif Halif, "Implikasi Yuridis Kebijakan Formulasi Alat Bukti Elektronik," *Lentera Hukum* 5, no. 2 (2018): 174, https://doi.org/10.19184/ejlh.v5i2.7469.

[12] Noor Rahmad et al., "Efektivitas Bukti Elektronik Dalam UU ITE Sebagai Perluasan Sistem Pembuktian Dalam KUHAP," *Prosiding 16th Urecol: Seri Pendidikan Dan Humaniora*, 2022, 96–111.

and can be accounted for so that it can explain a situation. The obligation to fulfill these legal requirements is absolute, as confirmed in Article 5 paragraph (3) of the ITE Law. If one of these conditions is not met, electronic evidence cannot be considered valid as evidence in court. This requirement is important because electronic evidence has different characteristics from non-electronic evidence, such as being easier to change, lose, or destroy.[13]

In addition to using procedures to test the validity of electronic evidence, it is important to adopt additional approaches to ensure that the evidence is not the result of AI technology.[14] Given the rapid advancements in artificial intelligence, it is increasingly difficult to distinguish between data that is authentic and that which has been manipulated by AI. Therefore, one of the steps that can be taken is to involve experts who have special expertise in digital forensics or information technology. For example, by involving an expert in the field of information and electronic transactions to analyze and verify the authenticity of electronic evidence. This expert is not only able to identify signs of manipulation or fabrication by AI, but can also provide in-depth testimony at trial on the methods used in the verification process. With their expertise, they can ensure that the evidence is truly authentic and not the result of sophisticated digital engineering techniques.

This process can be costly, especially since digital forensic analysis often involves sophisticated technology and in-depth knowledge. However, the investment in bringing in an expert can make or break a legal case. With verification from an expert, the electronic evidence submitted will have a stronger weight in the eyes of the judge and related parties, and reduce the risk of rejection of evidence due to doubts about its authenticity. In addition, expert involvement can also help in developing new standards in law enforcement related to electronic

---

[13] Rahmad et al.

[14] Hardianto Djanggih and Nurul Qamar, "Penerapan Teori-Teori Kriminologi Dalam Penanggulangan Kejahatan Siber (Cyber Crime)," *Pandecta: Research Law Journal* 13, no. 1 (2018): 10–23, https://doi.org/10.15294/pandecta.v13i1.14020.

evidence. With the development of technology, standards for verification and validation of electronic evidence need to be updated to keep up with the times. Experts involved in the legal process can play a role in providing recommendations and input for the formation of regulations that are more adaptive to new technologies, including artificial intelligence.[15] Electronic evidence can play a key role in determining whether a case can be dismissed by investigators or should proceed to the prosecution stage in court. During the trial process, the judge may use electronic evidence as clues to identify the crime. The judge will then seek the opinion of an expert, which will be included as expert testimony in the trial. Thus, rechtvinding by the judge becomes important, where the judge is expected to conduct an in-depth and logical evaluation in assessing the evidence. (effectiveness). Thus, the aforementioned measures not only strengthen the validity of electronic evidence in certain cases but also contribute to the development of a more robust and responsive legal system in accordance with the standards of validity and legal force established by Law Number 11/2008 on Electronic Information and Transactions and adapted to the challenges of the digital era.

B. AI Technology in The Indonesian Justice System

The transformation of legal culture in the digital age, with the integration of AI as a key component, offers significant potential to improve efficiency, accessibility and fairness in a country's legal system. Nonetheless, the use of AI in the legal decision-making process also faces significant challenges, which require careful handling. For this, society needs to understand and be aware of various crucial aspects, such as ethics, algorithms, data protection, and the need for adequate regulation. These critical issues require a careful approach for AI to function effectively as a tool for better and fairer legal decision-making, while maintaining the integrity and fundamental principles of the law.[16] In addition, challenges

---

[15] Djanggih and Qamar.

[16] Aan Setiadarma et al., "Tinjauan Literatur Transformasi Sosial Dalam Era Virtual," *Khatulistiwa: Jurnal Pendidikan Dan Sosial Humaniora* 4, no. 1 (2024): 232–44, https://doi.org/10.55606/khatulistiwa.v4i1.2930.

such as disinformation and data privacy must be handled sensibly, while the opportunities offered by social media can be utilized to drive positive social change and innovation in the legal system. The integration of AI in law, if done right, can strengthen people's trust in the legal system and ensure that the principle of justice remains the main foundation in every legal decision taken.

Legal regulations in Indonesia regarding AI technology are currently implicit and scattered across various laws, with no clear and specific provisions regarding prohibitions on its use.[17] This lack of clarity creates confusion in dealing with new technological developments such as AI. Nonetheless, in the context of electronic systems, the current regulation of AI is based on the ITE Law. This law defines AI as part of an electronic system, which is "a series of electronic devices and procedures in charge of preparing, collecting, processing, analyzing, storing, displaying, announcing, sending, and/or disseminating electronic information."[18]

Artificial intelligence (AI) is fundamentally different from human intelligence. Therefore, AI mechanisms for evidence generation need to be closely monitored to ensure compliance with the security standards that are prerequisites for its use, especially in the context of criminal justice. The main challenges related to the use of AI in this domain can be summarized in the following three aspects:

1. Unexplained

   AI is revolutionary in its applications and capabilities, however, with respect to its potential use in criminal justice, AI is functionally similar to traditional software: data in and conclusions out. In between, there is a 'black box' of calculations that not only are sometimes inaccessible to the experts themselves, but also few people in the courtroom

---

[17] BPPT, "Strategi Nasional Kecerdasan Artifisial Indonesia 2020 - 2045," *Badan Pengkajian Dan Penerapan Teknologi*, 2020, 194, https://ai-innovation.id/server/static/ebook/stranas-ka.pdf.

[18] Ekinia Karolin Sebayang, Mahmud Mulyadi, and Mohammad Ekaputra, "Potensi Pemanfaatan Teknologi Artificial Intelligence Sebagai Produk Lembaga Peradilan Pidana Di Indonesia," *Locus Journal of Academic Literature Review* 3, no. 4 (2024): 317–28, https://doi.org/10.56128/ljoalr.v3i4.311.

understand. Herein lies the danger of AI not properly being given the presumption of reliability, objectivity, and certainty, due to its mechanical appearance and seemingly simple output.[19] In order for a panel of judges or jurors to make an informed decision on the guilt of the defendant, light must somehow be shed on the black box. Moreover, given that AI outputs are often inexplicable, the question of how the defendant will be able to defend himself and challenge the evidence generated by it arises.

2. Discrimination and Bias

At the same time, decisions taken by algorithms may be generated from incomplete and therefore unreliable data: data may be tampered with by cyberattackers, biased, or incorrect. Applying emerging technologies without due consideration will therefore lead to outcomes that society is reluctant to accept their use by courts, as the risk of damage is always a distinct possibility. Thus, one of the toughest challenges to the successful incorporation of AI in criminal justice is the elimination of all types of biases to which AI is susceptible. Indeed, such biases can then lead to poor and unfair judicial decision-making, when taken into account by the bench or jury. In fact, all of these processes have hidden subjectivities and errors that often go unrecognized and unchecked, thus potentially 'facilitating the disguise of unauthorized or illegal discrimination behind layer upon layer of mirrors and proxies.[20]

3. Lack of accountablilty

Furthermore, when data is first collected or generated, human error in collection or interpretation is common.(Policing Criminal Justice Data) Human error can occur in the data training phase or even in further program development. However, in order to establish accountability, one needs to pinpoint the person behind the program, who made the mistake. In machine learning systems, where computer scientists often

[19] Andrea Roth, "Trial by Machine," *Georgetown Law Journal* 104, no. 5 (2016): 1245–1305.
[20] Omer Tene and Jules Polonetsky, "Judged by the Tin Man: Individual Rights in the Age of Big Data," *Jm* 4, no. April (2012): 1–55.

cannot determine how or why the machine learning system made certain decisions, this is very difficult to achieve.[21] In addition, one of the arguments in favor from the side of AI experts and AI companies is that AI systems and in particular machine learning are evolving in an unpredictable way, due to their autonomous and self-learning nature. As a result, no programmer can be held accountable for their evolution.

Criminal law has the primary objective of preventing harm and moral offenses arising from behavior prohibited by law. By establishing moral directives, criminal law enables offenders to be morally punished and threatened with appropriate criminal sanctions. However, technological advancements in the development of increasingly complex AI, or even creating highly intelligent artificial entities, pose great challenges to criminal law. One of the key factors in holding someone accountable for a crime is human control. When complex AI acts autonomously, human influence and control over it diminishes, creating a dilemma in determining who should be held accountable. In other words, the highly complex nature of AI often conflicts with the legal requirements for establishing criminal responsibility.[22]

The use of AI may cause confusion in determining liability, especially since the AI regulation in the ITE Law is not comprehensive enough to regulate AI in detail. This is important because the integration of AI technology in the legal domain should be done without using terms that can be interpreted differently. Arkha Dirata, in the "Policy Test Think Intergenerational Bridging The Solution of Today and Tomorrow" event cited by Hukum Online, stated that to regulate AI, standards are needed, as has been applied internationally. The first step for regulators in

---

[21]   John Buyers, *Artificial Intelligence: The Practical Legal Issues*, *Somerset: Law Brief Publishing* (Law Brief Publishing, 2018).
[22]   Eka Nanda Ravizki and Lintang Yudhantaka, "Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual Dan Tantangan Pengaturan Di Indonesia," *Notaire* 5, no. 3 (2022): 351–76, https://doi.org/10.20473/ntr.v5i3.39063.

developing AI regulations is to set standards for managing the AI system itself. Furthermore, it is important to establish a regulatory body that may be managed by the Ministry of Communication and Information Technology.[23]

The use of electronic evidence in criminal justice in Indonesia in the AI era offers various advantages, such as increased efficiency, accuracy, and availability of evidence. However, challenges related to validity, reliability, ethics, and regulation must be addressed to ensure that electronic evidence is admissible and lawfully used in court. It is important to continuously update regulations, improve law enforcement skills, and develop a solid ethical framework to face these challenges and optimally utilize the potential of AI in the justice system. While AI has great potential to streamline the judicial process, its success does not solely depend on the technology. AI implementation must be supported by various additional elements, such as clear regulations, training for legal professionals, and protection of individual rights. In addition, ethical aspects, data privacy, and transparency must also be considered. By integrating all these elements, AI technology can make a significant contribution in improving the efficiency of the criminal justice system while maintaining the principles of justice and human rights.

C. Evaluate the Power of Electronic Evidence in Criminal Proofing in Indonesia Effectively and Efficiently in the AI Era

Artificial intelligence (AI) has begun to be integrated into the criminal justice system in Indonesia with the aim of achieving aspirations of improved procedural fairness, economic efficiency and overall effectiveness. To realize these aspirations, a higher level of social acceptance of AI is required. However, for AI to be widely accepted, the technology must fulfill three key components that have been formulated by the HighLevel Expert Group on Artificial Intelligence (AI HLEG) :

1. Compliance with the law

---

[23] Sutri Anggita and Tamaulina Br. Sembiring, "Reformasi Sistem Peradilan Pidana Tantangan Dan Prospek Di Era Digital," *Journal of International Multidisciplinary Research* 2, no. 1 (2024): 256–71.

AI systems must comply with all applicable laws and regulations, ensuring that their use does not violate the principle of legality.

2. Compliance with ethics

AI should uphold ethical values and principles, ensuring that its use does not violate the moral norms of society

3. Technical and social resilience

AI must be designed with sufficient technical and social robustness to prevent unintentional harm from occurring, even if the intentions are good. [24]

Currently, AI systems used in legal contexts do not fully meet this standard of trust. Most AI systems have no built-in ability to explain or report on the decisions they make. In fact, the relevant scientific community broadly agrees that regulators should require developers to embed "explainability systems" in their AI solutions, especially when AI decisions can significantly impact individuals or regulations. According to the ethical guidelines for trustworthy artificial intelligence, also formulated by ai hleg, there are several key principles that ai systems must fulfill in order to be socially and ethically acceptable:[25]

a. Human control and supervision, AI systems must allow human supervision at every stage.

b. The technical resilience of AI must be robust and secure in the face of failure or manipulation.

c. Privacy and data governance, data protection should be a top priority.

d. Transparency, AI work processes and decisions should be understandable to users and affected parties.

e. Diversity, non-discrimination and fairness, the system should ensure fairness and avoid bias.

---

[24] Buyers, *Artificial Intelligence: The Practical Legal Issues*.
[25] Buyers.

f. Societal and environmental well-being, the use of AI should contribute to social well-being and environmental sustainability.
g. Accountability, there should be a clear mechanism to assign responsibility for the outcomes and impacts of AI decisions.

Trust in AI control mechanisms presents many regulatory challenges. Trust should not be an abstract or vague concept, but should be a reflection of clear, effective and operational regulations. This requires close collaboration between legal experts and AI experts. This cooperation aims to produce solutions that not only fit within the framework of legal practice, but also ensure fairness and efficiency. Thus, AI can be accepted and used responsibly in the criminal justice system.[26]

Given the rapid development of technology, including in terms of artificial intelligence and digital tools, periodic evaluation of existing regulations and procedures becomes crucial. New technologies can bring significant changes in the way evidence is collected, analyzed, and used in judicial processes, so it is essential to ensure that the legal system remains relevant and effective in dealing with these new challenges. Periodic evaluations should include a thorough review of all aspects of regulation and procedures related to the application of technology in the criminal justice system. These include, but are not limited to, a revision of the legislation governing electronic evidence, training for law enforcement, as well as renewed operational guidelines that can accommodate the latest technological innovations. These regulatory and procedural adjustments need to be done proactively so that the justice system can integrate new technologies in ways that support efficiency and accuracy without sacrificing the basic principles of justice and legal certainty. The evaluation process should also involve consultations with various stakeholders, including legal practitioners, technicians, academics, and civil society. This

---

[26] Eftychia Bampasika, "Artificial Intelligence as Evidence in Criminal Trial," *CEUR Workshop Proceedings* 2844 (2020): 133–38.

approach ensures that the proposed changes are not only oriented towards technological progress, but also consider the social and ethical impact of the application of technology in legal processes.

In addition, it is important to establish feedback mechanisms that enable law enforcement and the public to provide input on the effectiveness of existing regulations and procedures. These mechanisms can help identify and address problems that may arise in practice, as well as ensure that the justice system continues to adapt rapidly to technological change. With a systematic and inclusive approach in the evaluation and adjustment of regulations, Indonesia can ensure that the criminal justice system not only remains responsive to technological innovation, but also preserves integrity, justice, and legal certainty which are key pillars in the conduct of fair and effective justice.

Conclusion

Electronic evidence, now legally recognised as a tool of evidence in criminal justice, plays an important role in revealing the material truth in legal cases. Nevertheless, significant challenges remain, in assessing the validity and reliability of such electronic evidence. The judge must make a careful and thorough assessment to ensure that electronic evidence is truly reliable. Transparent and accurate proof processes are becoming crucial to guaranteeing justice, especially given the huge impact of the imposition of criminal sentences on human rights. Therefore, the courts must develop and adapt the procedures and evidence tools used to keep up with technological progress, including artificial intelligence technology. The adjustment aims to ensure that the justice system is capable of delivering optimal results in law enforcement. In this context, the role of the judge becomes crucial. The judge must be able to judge and consider the probative strength of the evidence presented with a high degree of rigour, so that substantive justice can be achieved. The courts must continue to strive to ensure that the use of modern technology in judicial processes does not sacrifice the fundamental principles of justice, but rather strengthen the efforts of fair and integrated law enforcement.

References

Aan Setiadarma, Ahmad Zaki Abdullah, Priyono Sadjijo, and Dwi Firmansyah. "Tinjauan Literatur Transformasi Sosial Dalam Era Virtual." *Khatulistiwa: Jurnal Pendidikan Dan Sosial Humaniora* 4, no. 1 (2024): 232–44. https://doi.org/10.55606/khatulistiwa.v4i1.2930.

Bampasika, Eftychia. "Artificial Intelligence as Evidence in Criminal Trial." *CEUR Workshop Proceedings* 2844 (2020): 133–38.

BPPT. "Strategi Nasional Kecerdasan Artifisial Indonesia 2020 - 2045." *Badan Pengkajian Dan Penerapan Teknologi*, 2020, 194. https://ai-innovation.id/server/static/ebook/stranas-ka.pdf.

Buyers, John. *Artificial Intelligence: The Practical Legal Issues. Somerset: Law Brief Publishing*. Law Brief Publishing, 2018.

Dahabreh, Fares. "The Continued Usage of Artificial Intelligence in the United Arab Emirates Public Sector Organisations: An Extended Information System Success Model," 2023, 1–287.

Djanggih, Hardianto, and Nurul Qamar. "Penerapan Teori-Teori Kriminologi Dalam Penanggulangan Kejahatan Siber (Cyber Crime)." *Pandecta: Research Law Journal* 13, no. 1 (2018): 10–23. https://doi.org/10.15294/pandecta.v13i1.14020.

Dmitrieva, A. A., and P. S. Pastukhov. "Concept of Electronic Evidence in Criminal Legal Procedure." *Journal of Digital Technologies and Law* 1, no. 1 (2023): 270–95. https://doi.org/10.21202/jdtl.2023.11.

Hartono, Sugi, Made, and Rai Yuliartini, Ni, Putu. "PENGGUNAAN BUKTI ELEKTRONIK DALAM PERADILAN PIDANA." *Nature Microbiology* 3, no. 1 (2020): 641. http://dx.doi.org/10.1038/s41421-020-0164-0%0Ahttps://doi.org/10.1016/j.solener.2019.02.027%0Ahttps://www.golder.com/insights/block-caving-a-viable-alternative/%0A???%0Ahttp://dx.doi.org/10.1038/s41467-020-15507-2%0Ahttp://dx.doi.org/10.1038/s41587-020-05.

Isima, Nurlaila. "KEDUDUKAN ALAT BUKTI ELEKTRONIK DALAM PEMBUKTIAN PERKARA PIDANA" 5, no. 1 (2022): 179–89.

Manope, Indra Janli. "Kekuatan Alat Bukti Surat Elektronik Dalam

Pemeriksaan Perkara Pidana." *Lex Crimen* Vol. VI No, no. Vol. VI/No. 2/Mar-Apr/2017 (2017): 107–13. https://ejournal.unsrat.ac.id/index.php/lexcrimen/article/view/1535 0/14898.

Prasetyo, Eko Surya, Y.A. Triana Ohoiwutun, and Halif Halif. "Implikasi Yuridis Kebijakan Formulasi Alat Bukti Elektronik." *Lentera Hukum* 5, no. 2 (2018): 174. https://doi.org/10.19184/ejlh.v5i2.7469.

Rahmad, Noor, Kuni Nasihatun Arifah, Deni Setiyawan, Muhammad Ramli, and Brian Septiadi Daud. "Efektivitas Bukti Elektronik Dalam UU ITE Sebagai Perluasan Sistem Pembuktian Dalam KUHAP." *Prosiding 16th Urecol: Seri Pendidikan Dan Humaniora*, 2022, 96–111.

Ravizki, Eka Nanda, and Lintang Yudhantaka. "Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual Dan Tantangan Pengaturan Di Indonesia." *Notaire* 5, no. 3 (2022): 351–76. https://doi.org/10.20473/ntr.v5i3.39063.

Roth, Andrea. "Trial by Machine." *Georgetown Law Journal* 104, no. 5 (2016): 1245–1305.

Sebayang, Ekinia Karolin, Mahmud Mulyadi, and Mohammad Ekaputra. "Potensi Pemanfaatan Teknologi Artificial Intelligence Sebagai Produk Lembaga Peradilan Pidana Di Indonesia." *Locus Journal of Academic Literature Review* 3, no. 4 (2024): 317–28. https://doi.org/10.56128/ljoalr.v3i4.311.

Sutri Anggita, and Tamaulina Br. Sembiring. "Reformasi Sistem Peradilan Pidana Tantangan Dan Prospek Di Era Digital." *Journal of International Multidisciplinary Research* 2, no. 1 (2024): 256–71.

Tene, Omer, and Jules Polonetsky. "Judged by the Tin Man: Individual Rights in the Age of Big Data." *Jm* 4, no. April (2012): 1–55.

***

DECLARATION OF CONFLICTING INTERESTS

FUNDING INFORMATION

ACKNOWLEDGMENT

HISTORY OF ARTICLE

About Author(s)

Benny Sumardiana, S.H., M.H., is a lecturer at the Faculty of Law, Universitas Negeri Semarang, where he teaches Criminal Law Procedure and Criminal Law Procedure Practice. He is actively involved in research and educational activities in Semarang and surrounding areas in Central Java Province. His research interests include criminal law, criminal law procedure, legal aid, and various other critical legal issues.

Prof. Dr. Pujiyono S.H., M.Hum., is a Professor at Universitas Diponegoro (UNDIP) in Central Java, Indonesia, and an expert in criminal law and criminal law procedure. His scholarly work has significantly contributed to the development of criminal law science. Recently, he has been involved as a drafting member of the latest Criminal Code, or Constitution number 1 of 2023.

Dr. Irma Cahyaningtyas S.H., M.H., completed her Doctoral program at the Faculty of Law, Universitas Diponegoro, and is currently a lecturer at the same faculty. She teaches Criminal Procedure Law, Special Criminal Procedure Law, Litigation Skills, Law on Confiscation, and Law on Military Courts. Her research is closely linked to her teaching subjects, and she often integrates her research findings into her lectures. For example, while teaching criminal law and child protection, she discusses the process of fostering children in correctional institutions, using her research in the field to enhance the learning experience.

This page intentionally left blank