Immutable Digital Timestamp as a Preventive Measure Against Podcast Manipulation: A Normative and Comparative Legal Analysis

Ninik Zakiyah[1], Budi Santoso[2], Muh. Afif Mahfud[3], Try Hardyanthi[4], Noor Kholifah Hidayati[5]

[1]Faculty of Law, Universitas Diponegoro, Indonesia
[2]Faculty of Law, Universitas Diponegoro, Indonesia
[3]Faculty of Law, Universitas Diponegoro, Indonesia
[4]Faculty of Law, University of Pécs, Hungary
[5]Faculty of Law, Universitas Muhammadiyah Purwokerto, Indonesia
✉ Corresponding email: ninikzakiyah@walisongo.ac.id

History of Article
Submitted : April 15, 2026
Revised : April 24, 2026
Accepted : May 10, 2026
Published : June 01, 2026
DOI : https://doi.org/10.37253/jjr.v28i1.12087

Abstract

The growth of digital audio content distribution through podcast platforms raises concerns about the authentication and integrity of electronic evidence within Indonesia's legal system. Although the ITE Law recognizes electronic information and documents as valid evidence, it has yet to establish clear technical standards for verifying the integrity and publication date of digital content. This article adopts a normative legal approach, using a comparative method to examine the United States and the European Union. In the United States, the authentication of electronic evidence under Federal Rule of Evidence Rule 901 generally accepts hash verification and chain of custody as reliable methods. Meanwhile, the European Union, through Regulation (EU) No. 910/2014 (eIDAS), has institutionalized qualified electronic timestamps as part of its trust services, providing a presumption of data integrity. This comparison shows that Indonesia still follows a reactive evidentiary model and has not yet implemented preventive technical standards. This article proposes a normative reconstruction that requires immutable timestamps and minimum hash standards for implementing regulations as a form of "regulation by architecture" and "compliance by design." This approach aims to improve legal certainty and accountability without impeding free expression, making the integrity of digital content an integral part of the national legal framework.

Keywords: Podcast; Immutable Digital Timestamp; Content Manipulation; Legal Analysis

Introduction

Digital transformation has shifted the paradigm of public communication from traditional broadcasting models to a digital platform-based distribution system (Marpi & Sunarno, 2025). Podcasts, as an on-demand audio medium, have become one of the fastest-growing forms of digital expression because of their flexibility in production and distribution. However, this flexibility introduces risks of manipulation through digital editing techniques, out-of-context editing of statements, and the reproduction of altered content (Zellatifanny, 2020). In Indonesian law, although electronic evidence is recognized by Law No. 11 of 2008 on Information and Electronic Transactions, as amended by Law No. 1 of 2024, there are no specific technical regulations to ensure the integrity of digital audio content (Ferdiyansah et al., 2025). The absence of such standards creates vulnerabilities for legal evidence when disputes arise over manipulated podcast content.

A study on electronic evidence in Indonesia conducted by Nurul Aini and Fauziah Lubis indicates a critical need to improve the effectiveness of evidence presentation in cybercrime cases. This is due to major challenges, including the complexity of cybercrime, anonymous perpetrators, the volatility of digital evidence, and limited resources (Aini & Lubis, 2024). Research by I Made Adnyana states that podcasts do not fall under the category of broadcasting and, under the ITE Law, remain a supplementary tool, creating legal uncertainty; thus, specific regulations are needed that are appropriate and that ensure freedom of expression as well as legal accountability (Adnyana & Liswahyuningsih, 2025). Furthermore, Astri Aprilianti's research, which focuses on her perspective on the ITE Law regarding technological advancements as the basis for legal certainty, still needs improvements to ensure justice and effectiveness (Aprilianti, 2024). Several other studies have addressed aspects of personal data protection on streaming platforms, but current literature remains reactive toward content

already published rather than preventative from a technical perspective regarding app usage.

Additionally, these studies have not specifically examined the integrity of digital audio podcast content as a target for manipulation, which directly impacts defamation and statement distortion. The discussion of defamation, copyright, and freedom of expression in this article is used only in a limited capacity as a normative context to clarify legal implications, while the primary focus of the analysis remains on the technical integrity of digital content and the construction of electronic evidence. In an international context, Lawrence Lessig, through the concept of "code as law," asserts that technological architecture can function as an effective regulatory tool (Lessig, 2006). Furthermore, Stephen Mason's (2018) research on digital evidence integrity emphasizes the importance of technical mechanisms to ensure the authenticity and integrity of digital evidence in court (Seng, 2018). In the United States, the Federal Rules of Evidence require the authentication of digital evidence through technical integrity verification (Federal Rules of Evidence, 2024). Meanwhile, in the European Union, the eIDAS Regulation (EU) No. 910/2014 encourages the use of electronic timestamping mechanisms to verify the authenticity of electronic documents (European Commission, 2021). However, neither of these approaches has been specifically applied to podcast platforms, a medium for audio distribution vulnerable to manipulation.

The main limitation of previous studies is the lack of attention to self-regulatory access controls as a crime-prevention tool. Most rely solely on content takedowns or user-reported content. This article seeks to address this gap by proposing a technical solution: an immutable digital timestamp, serving as a preventive legal instrument that systematically limits exposure to harmful content. Another gap in prior research is the absence of a normative framework that integrates technical standards for preventing audio manipulation into national legal systems. Regulations remain reactive and focus on enforcement after crimes occur rather than prevention through system design. Therefore, there is a need to develop technology-based preventive mechanisms that can be

embedded into the obligations of electronic system operators and integrated into digital platform architecture.

This article proposes an innovative approach by suggesting the implementation of immutable digital timestamps for each podcast episode as a form of regulatory architecture. These timestamps can act as indicators of content integrity and verification tools in cases of manipulation. Thus, the main novelty of this article lies in the integration of the concept of immutable digital timestamps with a "compliance by design" approach, specifically applied to the context of podcast platforms as objects of digital audio manipulation. This strategy not only strengthens legal protection for sources, the public, and podcast creators but also enhances the quality of evidence in criminal and civil cases involving digital audio content.

This study aims to analyze Indonesia's legal framework concerning the integrity of electronic evidence and the liability of electronic system operators, identify regulatory gaps in protecting against podcast content manipulation, compare international practices related to digital evidence integrity, and develop a model for implementing immutable digital timestamps as a preventive measure. The article is structured as follows: a normative legal methodology; a discussion of digital evidence integrity; an analysis of weaknesses in current regulations; a comparative analysis; and, finally, the normative construction of timestamps as a preventive tool solution.

Research Method

This study employs a normative legal research method (doctrinal legal research) with a prescriptive approach, which is a form of legal research that views law as norms enshrined in legislation and court decisions, as well as principles and doctrines developed in the legal literature (Marzuki, 2015). This approach is used to analyze normative gaps and weaknesses in the regulation of digital podcast content integrity and to formulate an appropriate legal framework regarding the application of immutable digital timestamps.

This study employs several approaches, including a legal approach, which involves analyzing the provisions of Law No. 11 of 2008 on Electronic

Information and Transactions (EIT Law), as amended by Law No. 19 of 2016; Law No. 1 of 2024; Law No. 32 of 2002 on Broadcasting (Broadcasting Law); the Criminal Code (KUHP); and the Criminal Procedure Code (KUHAP). This approach aims to identify how Indonesian positive law regulates the integrity of electronic evidence, the liability of electronic system operators, and criminal aspects related to defamation and information manipulation. A conceptual approach is also employed. This approach is intended to analyze the concepts of electronic evidence integrity, *digital evidence integrity*, *regulation by architecture*, *compliance by design*, and crime prevention. The conceptual approach is important because legislation has not yet explicitly regulated technical standards *for timestamps* on digital audio content, thus requiring a construction based on legal doctrine and theory. Furthermore, a comparative approach is also employed. This approach involves examining international practices regarding digital evidence integrity standards, including *timestamping* practices within electronic evidence management systems in jurisdictions that apply the *digital chain of custody* principle, including the US *Federal Rules of Evidence*, and the European Union's Regulation (EU) No. 910/2014, also known as the EU eIDAS Regulation. The selection of the United States and the European Union is based on their representativeness of the two main models in global electronic evidence governance. The United States represents an evidentiary-driven system in which integrity standards evolve through judicial practice and the doctrine of evidence. Conversely, the European Union represents a regulatory-institutional model, which explicitly integrates technical standards into a formal legal framework through the eIDAS Regulation. This comparison was then adapted to the Indonesian context, taking into account the compatibility of the legal system and institutional capacity.

The legal sources for this study include primary legal sources in the form of Indonesian laws and regulations; secondary legal sources, such as books, academic journals, and legal doctrines related to cyber law and electronic evidence; and tertiary legal sources, such as legal dictionaries and the digital legal encyclopedia (Syarif et al., 2024). The analysis was conducted prescriptively to formulate normative recommendations regarding the obligation to implement

immutable digital timestamps on podcast platforms as a preventive measure against content manipulation crimes.

Results and Discussions

Characteristics of Podcasts as Objects Vulnerable to Digital Manipulation

A podcast is digital audio content that is recorded, edited, and stored in a compressed file format, such as MP3 or WAV, and distributed via online platforms without geographical or national jurisdictional boundaries (Silaban et al., 2020). The main characteristics of podcasts lie in their *asynchronous* nature, the ability to be downloaded and reproduced without loss of quality (*lossless duplication*), and the ability to be modified using widely available, relatively accessible audio editing software (Sari & Rezeki, 2025). Unlike conventional live broadcasts, which are *real-time* and documented within a controlled broadcasting system, podcasts exist within a digital distribution ecosystem that is more fluid, fragmented, and lacks authoritative verification mechanisms.

In the context of criminal law, such actions may constitute defamation under the provisions of the Criminal Code (KUHP) or the Electronic Information and Transactions Law (ITE Law) (Nahor et al., 2025). However, the main issue lies not only in criminalization, but also in proving the authenticity of the audio content, specifically, that the circulating version has been modified from the original.

Technically, digital audio files represent sound waves as numerical data that can be reprocessed without leaving any visual traces of the changes. Unlike physical documents, which can show signs of deletion or correction, audio manipulation can be performed using techniques such as *cutting*, *splicing*, *overlaying*, *equalization*, and *time-stretching* without any obvious indication to the untrained listener (Sidabutar et al., 2025). In fact, recent advancements in AI-based *voice cloning* and *audio synthesis* technologies enable the reconstruction of voices that closely resemble the original speaker with high precision (Dewi &

Suyono, 2024). This situation makes podcasts inherently vulnerable to digital manipulation.

This vulnerability gives rise to at least three forms of manipulation risk. *First*, contextual truncation, which involves omitting certain parts of a source's statement, thereby significantly altering the context and meaning (Napoli, 2019). From a legal communication perspective, changes in context can shift the normative intent of a statement, so that a statement that was originally neutral or argumentative can be interpreted as an insult or a specific admission. *Second*, the rearrangement of audio fragments, which involves combining pieces of a statement to form a new narrative that the source never uttered in its entirety (Grigoras, 2005). *Third*, the distribution of edited versions for defamation, namely the dissemination of modified content with the intent to create a negative perception of a specific individual or institution (Rolph, 2025).

In Indonesian criminal law, such actions may constitute the criminal offense of defamation. The new Criminal Code, namely Law No. 1 of 2023 on the Criminal Code, retains provisions regarding insult and defamation as offenses against a person's honor and dignity. In addition, the ITE Law specifically regulates the distribution or transmission of electronic information containing insults or defamation through electronic systems (Ferdiyansah et al., 2025).

Article 27A of the ITE Law (Law No. 1 of 2024) stipulates that any person who intentionally distributes or transmits electronic information containing defamatory or libelous content is subject to criminal penalties. In the context of podcast manipulation, cutting or rearranging audio content and distributing it via digital platforms may satisfy the element of "distributing electronic information." However, the main problem lies in the proof: how to demonstrate that the circulating version has been modified from the original (Mufid & Hariandja, 2019).

Under Indonesia's legal system of evidence, admissible evidence is regulated in Article 184 of the Criminal Procedure Code (KUHAP), which includes witness testimony, expert testimony, documents, physical evidence, and the defendant's statement. With advances in technology, the Supreme Court has

recognized electronic evidence as an extension of documentary and physical evidence through various rulings. Article 5(1) of the ITE Law itself states that electronic information and/or electronic documents, along with their printouts, constitute valid legal evidence (Sariani, 2024). However, the admissibility of electronic evidence does not automatically resolve the issue of authenticity.

Authenticity is a central issue in cases involving podcast manipulation. If two audio versions are in circulation—the original and an edited version—the court must determine which one is the authentic recording. In practice, this proof relies on the testimony of a digital forensics expert who analyzes metadata, frequency spectra, *bitrate consistency*, and editing traces in the audio file. However, not all manipulations leave easily detectable technical traces, especially if the perpetrator uses professional software (Ariyaningsih et al., 2023).

Furthermore, this issue is also related to the principle *of chain of custody* in digital evidence law (Seng, 2018). Without a system for recording time and file integrity from the moment the content is recorded and published, claims regarding its authenticity become open to dispute. In this context, the urgency of an *immutable digital timestamp* mechanism becomes clear. By applying an unalterable timestamp to the original audio file, content creators can demonstrate that a specific version existed at a specific time and has not been altered since then. Conceptually, this mechanism can strengthen the evidentiary position in both criminal and civil disputes.

In addition to criminal law, podcast manipulation may also fall under civil law, specifically the tort of unlawful acts (Article 1365 of the Civil Code). If the dissemination of an edited version results in reputational harm, the loss of an employment contract, or other economic losses, the victim may seek damages based on the principle of *fault liability* (Setiawan & Khasanah, 2024). In this context, proving the causal link between content manipulation and the damages suffered is crucial.

Another equally important aspect is Copyright. Podcasts, as sound recordings, are protected under Law No. 28 of 2014 on Copyright. The creator or holder of related rights has the exclusive right to publish and reproduce the work. Unauthorized manipulation that alters the integrity of the work may be

viewed as a violation of moral rights, specifically the right to preserve the integrity of the work, as stipulated in Article 5 of the Copyright Law (Lesfandra et al., 2025). Thus, unauthorized editing not only constitutes defamation but may also infringe the creator's moral rights.

Several real-world cases in Indonesia demonstrate how edited audio or video clips can spark public controversy and legal proceedings. The dissemination of statements by officials or public figures taken out of context often causes social upheaval before an official clarification can be issued. This phenomenon demonstrates that podcasts' vulnerability to manipulation is not merely a technical issue but also has systemic implications for reputation, social stability, and public trust in digital information (Avianto, 2023).

Thus, the characteristics of podcasts as digital objects that are easily modified, replicated, and distributed without centralized control make them vulnerable to manipulation, with complex legal implications. The issue extends beyond the criminalization of such acts to the epistemological challenge of proving the authenticity of content within the judicial system. In this context, a preventive approach to strengthening digital integrity, including the implementation of *immutable digital timestamps,* becomes relevant to bridge the gap between the development of digital audio technology and the legal system's capacity to ensure certainty and protect rights.

The Integrity of Electronic Evidence and Issues of Proof

The recognition of electronic evidence in the Indonesian legal system represents a progressive development that aligns with the digital transformation. Article 5(1) of the ITE Law stipulates that electronic information and/or electronic documents, along with their printed copies, constitute valid legal evidence. This provision expands the evidentiary regime under Article 184 of the Criminal Procedure Code (KUHAP), which previously did not explicitly address electronic evidence (Baried, 2022). However, this normative recognition remains general and has not yet been accompanied by comprehensive technical standards for the integrity of digital content. The ITE Law does not explicitly require

electronic system operators to provide a public audit trail mechanism, post-publication file integrity verification, or an unalterable timestamping system. The absence of these technical standards creates a gap between the formal recognition of electronic evidence and the legal system's practical ability to verify its authenticity (Aini & Lubis, 2024).

In modern evidence law, there is a conceptual distinction between *admissibility* (the acceptability of evidence) and *authenticity* (the integrity or authenticity of evidence) (Vanessa & Firmansyah, 2025). The ITE Law has addressed admissibility but has not yet fully regulated the technical aspects of authenticity. Article 6 of the ITE Law requires that electronic information be considered valid so long as a reliable and secure electronic system generates it. However, the phrase "reliable and secure" is not elaborated upon in the uniform operational standards.

Article 5(1) of the ITE Law stipulates that electronic information and/or electronic documents, along with their printed copies, constitute valid legal evidence. This provision expands the evidentiary regime under Article 184 of the Criminal Procedure Code, which previously did not explicitly mention electronic evidence. Furthermore, Article 6 of the ITE Law requires that electronic information be considered valid provided it is generated using a reliable and secure electronic system. The provisions of Article 5 and 6 of the ITE Law implicitly support the principle of electronic system integrity, but do not yet provide measurable technical parameters, thereby creating a normative gap in implementation, particularly in ensuring the integrity and authenticity of digital content. This creates a normative gap in implementation, particularly due to the absence of technical standards that can be objectively tested in the evidentiary process.

Regarding the manipulation of podcast audio, authenticity is central. If an audio file has been edited by cutting or rearranging fragments, the file technically remains an electronic document that can be submitted as evidence (Lubis et al., 2025). Problems arise when two versions are in circulation, and the court must determine which is the authentic recording. Without a preventive digital integrity system, judges will rely on ex post facto forensic evidence.

In judicial practice, proving the authenticity of electronic files typically relies on the testimony of a digital forensics expert, who analyzes frequency spectra, *waveform consistency*, *hash values*, and potential editing traces. File metadata includes information such as creation time, last modification time, device used, and file compression structure. Additionally, server or distribution platform logs can indicate the upload time, IP address, and history of changes (Insa, 2007).

Although these three tools do not fully guarantee integrity, metadata can be modified using certain software. Server logs depend on the platform's data retention policies, which are not always transparent or publicly accessible. In fact, in some cases, logs may be automatically deleted after a certain period in accordance with the internal policies of the electronic system operator. As a result, proving the facts becomes complex and costly. Hiring digital forensic experts entails high costs, while not all parties have access to such resources (Casey, 2011). This situation has the potential to create *an inequality of arms* in the judicial process.

The lack of clarity regarding digital integrity standards creates three main implications: *First*, legal uncertainty; without preventive technical standards, each case will rely heavily on expert interpretation and judicial discretion. Rulings may be inconsistent because they depend on the quality of the forensic analysis in each case. *Second*, prolonged debates over the authenticity of evidence; disputes often shift from the substance of defamation to technical debates over whether a file has been manipulated. This prolongs the trial process and reduces the efficiency of the judicial system. *Third*, the high cost of proof: the aggrieved party must fund forensic examinations to prove that the content has been modified (Nurullah, 2024). This situation has the potential to hinder access to justice, especially for individuals with limited resources.

Conceptually, the Indonesian legal system remains focused on *post-crime verification* that is, verifying integrity after a dispute arises—rather than on *pre-crime integrity assurance*, which involves prevention through a system that ensures integrity from the very beginning of publication (Sriwidodo, 2019).

Any regulatory intervention regarding digital platforms must take into account the constitutional guarantee of freedom of expression as stipulated in Article 28F of the 1945 Constitution. This article guarantees every person's right to communicate and obtain information through various available channels. However, freedom of expression is not an absolute right. Article 28J of the 1945 Constitution stipulates that the exercise of human rights may be restricted by law to the extent necessary to ensure the recognition and respect for the rights of others and to meet the demands of justice in accordance with moral considerations, religious values, security, and public order.

The Constitutional Court has affirmed in various rulings that restrictions on freedom of expression must comply with the principle of legality—meaning that restrictions must be based on law—as well as the principle of legitimate aim, which seeks to protect the rights of others or the public interest, and the principle of Proportionality, whereby restrictions must be proportionate and not excessive (Konstitusi, 2008).

The requirement for *an immutable digital timestamp* does not restrict content or expression, but rather ensures the integrity of distribution. It does not prohibit anyone from speaking or publishing opinions, but ensures that published content has a verifiable timestamp and integrity. Therefore, such a measure can be classified as a proportional and constitutionally valid administrative restriction. *An immutable digital timestamp* is a mechanism that cannot be altered once attached to an electronic document. Technically, this mechanism can be implemented through cryptographic hash systems or *distributed ledger* technology. With this system, every published podcast audio file will have a unique *hash value* recorded at a specific time. If the file is altered, or even a single second of audio is cut, the hash value will change significantly. This mechanism provides objective proof of integrity that does not rely on manipulable metadata. From a legal evidentiary perspective, this system functions as a *self-authenticating evidence* tool, as its integrity can be verified without relying entirely on expert testimony. This has the potential to reduce evidentiary costs, enhance legal certainty, expedite court proceedings, and minimize technical disputes regarding authenticity(Insa, 2007). To align with

constitutional principles, the requirement for *immutable timestamps* can be designed as an obligation for operators of large-scale electronic systems, implemented gradually based on risk categories, subject to administrative oversight by the relevant ministry, and enforced through administrative sanctions rather than criminal penalties. With such a design, state intervention remains proportional and does not chill freedom of expression.

Immutable Digital Timestamp as a Preventive Mechanism

An immutable digital timestamp is a cryptographic mechanism attached to an electronic document or digital file that prevents tampering without being systematically detected. Technically, this mechanism works by *generating a hash value* a unique alphanumeric representation of a file, which is then recorded along with specific time information on a protected system. Even the slightest change to the file results in a significantly different *hash value*, allowing the document's integrity to be objectively verified (Menezes et al., 1996).

Unlike conventional metadata, which can be modified with specific software, *immutable timestamps* are designed to create an integrity trail independent of the user's local system. Timestamps can be implemented through several technical approaches, including: *Server-side cryptographic hashing*, which is the process of generating a hash by the server hosting the electronic system when a file is first uploaded; *Blockchain-based timestamp ledger*, which involves recording a hash on *a distributed ledger* that is decentralized and cannot be altered without network consensus and *Secure audit trail system*, which is an encrypted change-logging system that cannot be modified without leaving a forensic trail (Nakamoto, 2018).

Legally, the primary function of an immutable digital timestamp is not to restrict content, but to ensure the integrity and accountability of digital information distribution. In the context of legal evidence in Indonesia, this mechanism is highly relevant, as it can strengthen the *chain of custody* of electronic evidence (Baried, 2022). As outlined in the previous subsection,

Article 5(1) of the ITE Law recognizes electronic information and/or electronic documents as valid legal evidence. However, this recognition requires that the electronic system used must be reliable and secure (Article 6 of the ITE Law) (Pradipa, 2025). Problems arise when the standards of "reliability and security" are not elaborated upon in measurable technical indicators. An immutable digital timestamp can serve as a concrete parameter for assessing the reliability of an electronic system in ensuring the integrity of a document from the moment of its initial publication.

The authenticity of electronic evidence in judicial practice is often verified by forensic experts (Nurullah, 2024). Without preventive mechanisms, the verification process will always be reactive (*ex post*). Immutable timestamps shift this paradigm to a preventive (*ex ante*) approach, as integrity has been verified from the outset. Thus, judges do not rely solely on expert opinions; they can also conduct objective verification through hash value comparison. Conceptually, this aligns with the principle of legal certainty (*rechtszekerheid*), a fundamental principle of the Indonesian legal system. With a standardized timestamp system, the parties have certainty regarding the authenticity of electronic documents and do not need to engage in prolonged technical debates regarding the possibility of manipulation.

Nevertheless, the immutable digital timestamp mechanism is not entirely free from limitations. Some challenges that may arise include the potential for manipulation prior to the hashing process, reliance on reliable technical infrastructure, and the need for credible verification authority governance. Furthermore, the implementation of this mechanism also has implications for the operational costs of electronic system operators. Therefore, its implementation must be accompanied by clear operational standards and adequate institutional oversight to avoid creating new risks in digital governance.

For example, a guest on a 60-minute podcast voices criticism of a public policy. The criticism is presented in a reasoned and contextual manner. A certain party then cuts out a 30-second segment of the statement and circulates it separately, creating the impression that the guest made an extreme or provocative statement. Without an immutable timestamp system, the original and edited

versions could circulate simultaneously without an objective indicator of which was published first; metadata could be modified; courts would have to rely on complex digital forensic examinations; and the cost of proving the facts would increase, leading to lengthy trials.

Conversely, with an immutable timestamp system, the hash of the original file uploaded at a specific time is permanently recorded. Any modified file produces a different hash. Verification can be performed independently without requiring subjective technical interpretation. The verification process becomes faster and more efficient. In the context of criminal law, this mechanism strengthens the evidence for the element of "intentionally distributing electronic information containing defamatory content" as stipulated in the ITE Law. If it is proven that the distributed file differs from the original hash recorded, there is strong evidence of manipulative intervention.

The concept *of the chain of custody* refers to the chronological documentation of who has possessed, accessed, or modified a piece of evidence from the time it was first created until it was presented in court (Casey, 2011). In digital cases, *the chain of custody* is often a weak point because files can be easily copied and modified without a clear trail. An immutable timestamp strengthens *the chain of custody* by providing an unalterable initial integrity reference. Any changes can be tracked through hash comparisons. Thus, the timestamp serves not only as a time indicator but also as a systemic foundation for the integrity of electronic evidence.

As previously discussed, Article 28F of the 1945 Constitution guarantees freedom of expression and the right to access information. However, Article 28J permits restrictions provided they are prescribed by law and aim to protect the rights of others. The obligation to apply an immutable timestamp does not restrict the substance of expression, but rather ensures the technical integrity of distribution. It does not dictate what may or may not be said, but ensures that the authenticity of what is published can be verified. Thus, this policy can be classified as an administrative restriction that meets the proportionality test because, in terms of legality, it can be regulated through amendments to the ITE Law or subordinate regulations; it serves a legitimate aim of protecting reputation

and the right to honor; and it is proportional, as it does not restrict the content of expression but only the technical aspects of integrity.

This approach is also consistent with *the precautionary principle* in digital technology regulation, which aims to prevent harm before disputes arise. In the context of Indonesia's public policy (Daeng et al., 2023), the implementation of immutable timestamps can be designed through several approaches, including technical standardization by the government via a Ministerial Regulation on Communications and Digital Affairs regarding content integrity obligations for certain electronic system operators, followed by a risk-based approach applicable only to platforms with a large user base or distribution, further compliance incentives, such as certification for electronic systems meeting integrity standards; and administrative sanctions rather than criminal penalties to ensure Proportionality. With such a design, the state avoids overcriminalization while strengthening digital integrity governance. From a judicial system perspective, immutable timestamps have the potential to reduce the caseload related to authenticity disputes, accelerate the evidentiary process, lower the costs of expert testimony, and improve the consistency of rulings. With the presence of an objective indicator in the form of a hash value recorded at a specific time, judges have a more stable technical basis for evaluating electronic evidence.

An immutable digital timestamp is not merely a technical innovation, but a normative instrument capable of bridging the gap between advancements in digital audio technology and Indonesia's legal system of evidence. In the context of podcast manipulation, this mechanism serves as a guarantor of the integrity of the original publication, a detector of post-publication changes, a reinforcement of the chain of custody, and a preventive tool that reduces reliance on costly forensic evidence. Thus, immutable timestamps can be positioned as a preventive mechanism that is proportionate, constitutional, and aligned with the principle of legal certainty within Indonesia's legal system. Thus, immutable timestamps are not presented as an absolute solution, but rather as a preventive measure that requires adequate regulatory and technical ecosystem support.

Regulation by Architecture and Compliance by Design

Lawrence Lessig first popularized the idea that digital system architecture can function as a regulatory instrument through the concept *of "code is law*." In Lessig's view, behavior in cyberspace is governed not only by formal law but also by social *norms*, the *market*, and architecture or code (Lessig, 2006). System architecture, that is, the technical design and structure of software, can more effectively limit, direct, or enable user behavior than the threat of legal sanctions alone.

In the context of podcast manipulation, the implementation of *immutable digital timestamps* on audio distribution platforms can be understood as a form of regulation by architecture, since legal norms regarding integrity and accountability are no longer enforced solely through criminal penalties after a violation occurs, but are instead embedded within the technical design of the system itself. In other words, regulation is embodied in the technology's structure.

According to Lessig, code has coercive power because it determines what is and is not possible within a system (Lessig, 2006). If a platform is designed without integrity verification mechanisms, then content manipulation becomes relatively easy to carry out undetected. Conversely, if a system is designed with mandatory cryptographic hashing and tamper-proof timestamping, then the scope for manipulation is structurally narrowed.

This approach is relevant to Indonesian law because the legal system still faces challenges in establishing the authenticity of electronic evidence. As stipulated in Law No. 1 of 2024 on the Second Amendment to the Law on Information and Electronic Transactions (ITE Law), electronic information is recognized as valid evidence (Baried, 2022). However, the EIT Law has not yet incorporated technical integrity standards into the design requirements for electronic systems. By implementing immutable timestamps as part of the podcast platform's architecture, the state not only expands legal norms but also transforms them into technical mechanisms that operate automatically without requiring intervention from law enforcement.

The concept of compliance by design refers to an approach in which legal compliance is achieved not through the threat of sanctions, but through system

design that inherently encourages or enforces compliance. This approach is widely used in data protection regulations, for example, through the *"privacy by design"* principle (Cavoukian, 2011). In the context of podcasts and audio manipulation, "compliance by design" means that platforms must integrate integrity verification mechanisms from the outset of publication. Thus, every uploaded file automatically receives a unique hash. This hash is recorded in an immutable system. Any change results in a detectable systemic trace. This approach shifts the law enforcement paradigm from a repressive model (post-crime sanction) to a preventive model (pre-crime integrity assurance). In modern criminal policy, this shift is viewed as more efficient because it reduces the burden on law enforcement and minimizes losses before they occur.

The theory of situational crime prevention, developed by Clarke, emphasizes that crime can be reduced by modifying situations or environments so that opportunities to commit crime are reduced (Clarke, 1997). This approach does not focus on changing offenders' moral character, but rather on reducing opportunities. Within this framework, an immutable timestamp functions as a situational prevention tool by increasing the risk of detection for any manipulation—which would produce a different, verifiable hash—thereby reducing the likelihood of undetected manipulation since changes cannot be made covertly, and creating a system of accountability, wherein each version of the content possesses a cryptographic identity that can be compared.

If perpetrators know that any changes will be objectively detected, the incentive to engage in manipulation decreases. This approach aligns with preventive criminal policies that emphasize *reducing opportuniti*es for crime rather than harsher penalties (Widianingrum, 2024). Within the Indonesian legal system, preventive approaches have been established in various fields, including administrative law and consumer protection. However, in the context of cyber law, regulations remain predominantly repressive, particularly through the criminal provisions in the ITE Law. The application of "regulation by architecture" can serve as a complementary measure to strengthen the effectiveness of legal norms without expanding criminalization. This principle aligns with the "ultimum remedium" principle in criminal law, which holds that

criminal sanctions are used as a last resort after other mechanisms prove ineffective.

Furthermore, this approach is consistent with Article 28J of the 1945 Constitution, which permits restrictions on rights provided they are established by law and aim to protect the rights of others. The obligation of technical integrity does not restrict the substance of expression, but rather ensures the accuracy and authenticity of distribution. Therefore, it complies with the principles of legality and Proportionality. From a public policy perspective, the obligation for an immutable timestamp can be incorporated into regulations derived from the ITE Law through government regulations on electronic system integrity standards, ministerial regulations governing technical obligations for specific electronic system operators, and compliance certification schemes for digital platforms. Thus, legal norms are not merely declaratory but also operational in system design.

The "regulation by architecture" approach also encompasses the ethical dimension *of digital governance*. In an era of disinformation and content manipulation, digital platforms play a central role in shaping the public sphere. System integrity is part of the social responsibility of digital corporations. By mandating "compliance by design," the state encourages platforms not merely to act as neutral distribution channels, but also to serve as actors that share responsibility for safeguarding the authenticity of content. This approach is not synonymous with censorship, but rather with enhanced technical accountability. From an efficiency perspective, "regulation by architecture" can reduce disputes over authenticity, lower the costs of proof, expedite judicial processes, and enhance the consistency of rulings. If integrity is ensured through system design, the judiciary's focus can return to the substance of the case rather than technical debates over the authenticity of files (Novita et al., 2024).

Regulation by architecture and compliance by design offer a regulatory paradigm that adapts to advancements in digital technology. In the context of podcast manipulation, the requirement for an immutable timestamp embeds legal norms into technical design, reduces the likelihood of crime through a situational approach, strengthens the integrity of electronic evidence, aligns with

constitutional principles and the principle of ultimum remedium, and supports modern preventive criminal policies. Thus, this approach is not merely a technical innovation but a transformation of the digital regulatory paradigm, shifting the focus from punishment to prevention through system design.

Comparative Analysis: The United States and European Union

A comparative analysis is necessary to assess the extent to which Indonesia's legal system has integrated technical standards for the authentication of digital evidence compared to other jurisdictions that are more advanced in the governance of electronic evidence. The United States and the European Union were selected because both have relatively mature regulatory frameworks for digital evidence and the integration of technical mechanisms into their legal systems (Lukito, 2022).

In the United States, the authentication of digital evidence is governed by *the Federal Rules of Evidence* (FRE), specifically Rule 901. Rule 901(a) states that, to satisfy the requirements for authentication, the party presenting the evidence must produce sufficient evidence to support the finding that the item is what the party claims it to be (Kerr, 2009). This provision is principled and flexible, but federal judicial practice has developed fairly consistent technical standards for digital evidence. Rule 901(b) provides examples of authentication methods, including through the testimony of a knowledgeable witness, evidence of distinctive characteristics, and processes or systems that produce accurate results.

In the context of digital files, authentication is often performed by verifying hash values. Cryptographic hashes such as the Message Digest Algorithm (MD5) or the Secure Hash Algorithm (SHA-256) are used to demonstrate that the submitted file is identical to the original file that was seized or recorded. Federal courts consistently accept hash verification as a reliable method for ensuring file integrity. Digital forensic experts testify to the process of file acquisition and verification, including pre- and post-analysis hash matching. Audit trails and

chains of custody, with detailed documentation of who accessed or moved the evidence from the outset (Federal Rules of Evidence, 2024). In *United States v. Bonallo* (1988), the court admitted computer data as evidence because there were assurances of the system's reliability and no indication of unauthorized alteration (Federal Rules of Evidence, 2024). In modern practice, hash verification has become a standard part of digital forensic procedures, even before a case is filed in court.

A significant development occurred with the 2017 amendment to FRE Rule 902, which permits *self-authentication* for certain electronic data. Rules 902(13) and 902(14) allow for the self-authentication of electronic records generated by a reliable process or system, including through hash certification by a forensic expert (Federal Rules of Evidence, 2024). This means that if the hash value is verified and certified in accordance with procedures, the court no longer requires direct expert testimony for the initial authentication stage. This indicates that the US legal system has integrated technical mechanisms into formal evidentiary procedures.

In practice, *the chain of custody* plays a crucial role in the U.S. Every transfer of digital evidence must be documented in detail. If there are significant gaps in the documentation, the evidence may be challenged or even deemed inadmissible (Casey, 2011). This approach emphasizes both procedural and technical integrity. Thus, evidentiary standards in the US depend not only on judicial interpretation but also on standardized and documented forensic protocols.

Immutable digital timestamps align with hash verification practices in the US. In fact, if systematically implemented on podcast platforms, these timestamps can serve as a *pre-authentication* mechanism. When disputes arise, the initial hash is already available and documented, thereby simplifying authentication. Compared to Indonesia, the US system is more advanced in institutionalizing technical standards within formal evidentiary rules, rather than relying solely on expert practice

The European Union has adopted a different approach through Regulation (EU) No 910/2014 on electronic identification and trust services (eIDAS) (European Commission, 2021). This regulation governs digital trust services,

including electronic signatures, electronic seals, and electronic time stamps. Article 41 of eIDAS stipulates that *qualified electronic time stamps* have legal effect and cannot be rejected as evidence solely because they are in electronic form. These time stamps provide *a presumption of accuracy* regarding the date and time as well as the integrity of the associated data. Electronic time stamps under the eIDAS regime bind a specific time to electronic data, guaranteeing that the data has not changed since that time, and are legally recognized throughout all member states of the European Union.

Timestamps that meet the eIDAS standards must be issued by *a qualified trust service provider* (QTSP). These providers are subject to strict technical standards and oversight, including security audits and cryptographic certification. With this model, the European Union not only recognizes electronic evidence but also institutionalizes technical integrity through a formal regulatory framework. Integrity is not merely an issue of proof in court but a component of *the digital* trust *ecosystem*. The strength of the European Union's model lies in *its legal presumption*. If a document bears a qualified electronic timestamp, it is legally presumed that the data has not been altered since the recorded time, unless proven otherwise (Dumortier & Vandezande, 2012). This presumption reduces the burden of proof and enhances judicial efficiency. This mechanism is far more progressive compared to Indonesia's approach, which still relies entirely on ex post proof through expert testimony.

In Indonesia, the admissibility of electronic evidence is governed by the ITE Law. However, there are no national standards regarding hash-based integrity verification; there is no presumption of an integrity mechanism like eIDAS; the chain of custody is not formally regulated in evidentiary rules; and authentication remains heavily dependent on judicial interpretation and expert testimony. Here is a comparison of Indonesia, the United States, and the European Union:

Aspect	Indonesia	United States	European Union
Recognition of Electronic Evidence	Regulates under ITE Law	FRE Rule 901 & 902	eIDAS Regulation
Technical Hash Standards	Not specified	Recognized and standardized in practice	Integrated into trust services
Timestamp Regulated	Not regulated	Not explicit but accepted in practice	Regulated under eIDAS
Chain of Custody	No national standardized	Strict and documented	Integrated into the trust ecosystem
Self-authentification	There is no specific mechanism	Provided under Rule 902 (13)-(14)	Legal presumption of accuracy

Based on the table, it can be inferred that Indonesia still lacks technical standards for the integrity of electronic evidence. Indonesia recognizes electronic evidence normatively, but has not yet incorporated technical mechanisms into a formal regulatory framework.

Learning from the US and the European Union, there are two approaches Indonesia can adopt: a procedural model like the US, which involves integrating hash verification and self-authentication into procedural law, and a regulatory model like the European Union, which regulates electronic timestamps as a trust service with a presumption of integrity. Immutable digital timestamps on podcast platforms could serve as a first step toward such technical integration. By mandating hash-based timestamps at publication, Indonesia can strengthen its evidentiary system without waiting for major reforms to criminal procedural law. The United States emphasizes technical integrity through established evidentiary

procedures and forensic standards. The European Union institutionalizes integrity through trust services regulations that provide a legal presumption. Indonesia, although it has recognized electronic evidence, does not yet have equivalent technical standards. Therefore, the implementation of immutable digital timestamps in podcast platform regulations in Indonesia is a progressive step toward standardizing the integrity of electronic evidence while strengthening legal certainty and judicial efficiency.

Normative Framework and Regulatory Design for Digital Content Integrity within the Indonesian Legal System

The integrity of digital content is not merely a technical issue, but a matter *of the rule of law in the digital space*. In the context of evidence, modern legal systems recognize that electronic evidence must meet authentication and reliability standards to be admissible in court (Lubis et al., 2025). In the United States, these standards are outlined in Federal Rule of Evidence 901, which requires sufficient evidence to support a claim of authenticity for a digital document (Federal Rules of Evidence, 2024). Meanwhile, the European Union, through Regulation (EU) No. 910/2014 (eIDAS), explicitly institutionalizes *qualified electronic timestamps* as part of *trust services* that possess legal evidentiary weight (European Commission, 2021). Unlike these two regimes, Indonesia, through Law No. 1 of 2024 (Second Amendment to the ITE Law), does recognize electronic information as valid evidence, but has not yet specifically regulated technical integrity standards such as hash verification or state-verified timestamps. The absence of these national technical standards creates an excessive reliance on judicial interpretation and expert testimony, resulting in legal certainty that is relative and inconsistent.

Based on a comparative approach, the proposed regulatory model is multi-tiered; specifically, at the legislative level, explicit provisions must be added requiring electronic system operators (ESOs) to maintain the integrity of public content through publication time verification mechanisms, data integrity

verification mechanisms, and documentation of content changes (versioning logs). In the United States, although not specifically regulated in a single technology law, the obligation to maintain the integrity of evidence arises from evidentiary practices and authentication standards under FRE Rule 901 (Mueller & Kirkpatrick, 2025). In other words, the US system establishes the obligation of integrity through the doctrine of evidence. The European Union takes a different approach: eIDAS establishes a presumption of accuracy for *qualified timestamps*. This means the burden of proof shifts to the party challenging its validity (European Commission, 2021).

Indonesia could adopt a hybrid approach by incorporating normative recognition into the ITE Law, stipulating that digital content accompanied by a certified timestamp mechanism is *presumed to be intact*. At the technical-operational level, minimum standards, such as the Cryptographic Hash Standard—the Secure Hash Algorithm (SHA-256)—should be established, as recommended by the National Institute of Standards and Technology. Secure Timestamp Authority. This model can emulate the structure of *Trusted Service Providers* under the eIDAS regime. Timestamp service providers must be certified by a national authority. A public verification mechanism allows the public to verify hashes through an official portal. Minimum 5-Year Audit Log Retention refers to the *chain-of-custody* practices in the US evidentiary system (Casey, 2011).

In Indonesia, secondary regulations, such as Government Regulations (PP) or Ministry of Communication and Information Technology Regulations (Permen Kominfo), can address these technical details without burdening the legislative process. Technically, the proposed mechanism for podcast platforms could include hashing audio files upon publication, storing the hashes on distributed servers or blockchain-based systems, publishing hash references on episode pages, and providing a public verification feature. This model aligns with the "*integrity by design*" principle developed in modern information security governance. Here is a comparison:

Aspect	Indonesia (proposed)	United States	European Union
Presumption of Integrity	Requires regulation	Based on the burden of proof	Regulated through eIDAS
Hash Standard	Regulated by ministerial regulation	Based on best practice	Certified
Timestamp Authority	National	Decentralized	Qualified Trust Service

When assessed against the principles of human rights restrictions, the legitimate aim of this policy is to protect reputation, prevent content manipulation, and ensure legal certainty. This aligns with the permissible restrictions under Article 19(3) of the International Covenant on Civil and Political Rights (ICCPR). Regarding Necessity, there are no less restrictive alternatives capable of ensuring the integrity of evidence other than technical mechanisms for time and hash verification; and regarding Proportionality, this policy does not censor content, filter topics, or restrict distribution; it only regulates technical integrity. In the Indonesian context, the Constitutional Court has consistently emphasized the importance of Proportionality in the restriction of digital rights (Constitutional Court Decision No. 20/PUU-XIV/2016).

Indonesia currently still follows a reactive approach, in which integrity is tested only when disputes arise. The proposed model is preventive, similar to the European Union's approach to building *a digital trust ecosystem*. This can be seen in the following systemic comparison:

Model	Characteristic
Indonesia (currently)	Reactive-dispute-based
United States	Evidence-driven
European Union	Regulatory-institutional

Model	Characteristic
Indonesia (proposed)	Preventive-integrity-based

To ensure that this regulatory framework does not remain merely conceptual, concrete institutional designs and operational mechanisms are required, including: oversight may be assigned to the Ministry of Communication and Digital Affairs as the primary regulator of electronic system operators, with support from independent certification bodies for technical aspects; podcast platform operators are required to obtain electronic system integrity certification covering the implementation of hash verification, secure timestamping, and audit log systems. This model may adopt the trust service provider scheme as in the eIDAS regime; obligations are applied using a risk-based approach, prioritizing platforms with a large user base or broad distribution impact; violations of integrity obligations are subject to graduated administrative sanctions, ranging from a warning, administrative fines, to service restrictions, without immediately resorting to criminal instruments; to prevent overregulation, this mechanism does not regulate or restrict content substance, but only technical integrity aspects, thereby remaining consistent with freedom of expression within the constitutional framework. With this operational design, the integrity obligation is not only normative but also implementable and measurable in the practice of electronic system governance in Indonesia.

An immutable timestamp policy can enhance public trust, reduce the burden of proof in court, ensure transparency regarding content changes, and support a credible digital economy ecosystem. In the context of legal theory, this model shifts the approach from *"trust the speaker"* to *"trust the system*." This normative reconstruction model positions technical integrity as an integral part of legal certainty. By adopting US evidentiary practices and institutionalizing EU trust services, Indonesia can build a more objective, standardized, and constitutionally grounded system for electronic evidence. Immutable timestamp regulation is not a tool for censorship, but rather a tool for accountability.

Conclusion

This study demonstrates that the recognition of electronic evidence in the Indonesian legal system has not been accompanied by adequate technical standardization to ensure the integrity of digital content. Although Law No. 1 of 2024 has affirmed electronic information and documents as valid legal evidence, the regulation does not explicitly address technical authentication mechanisms such as cryptographic hash verification or immutable digital timestamps. Consequently, proving the integrity of content—including on podcast platforms—still relies on judicial interpretation and expert testimony, thereby creating legal inconsistency and uncertainty. A comparison with the United States and the European Union reveals significant differences in regulatory models. In the United States, the authentication of digital evidence is governed by Federal Rule of Evidence Rule 901, which requires proof that a document is what it claims to be. Federal judicial practice has accepted methods such as hash verification, audit trails, and chain of custody as reliable means of ensuring the integrity of digital files. Although there is no national requirement regarding certified timestamps, technical standards have been internalized within evidentiary practice. Conversely, the European Union, through Regulation (EU) No. 910/2014 (eIDAS), has institutionalized *qualified electronic timestamps* as part of *trust services* that provide a presumption of accuracy regarding the time and integrity of electronic data. This model demonstrates a preventive, structured approach to building *a digital* trust *ecosystem*, so that technical integrity is not merely an evidentiary issue but an integral part of formal regulatory design.

From this comparative analysis, it can be concluded that Indonesia still operates under a reactive evidentiary model (*ex post evidentiary model*). To address this regulatory gap, this study proposes a multi-tiered regulatory framework: (1) the inclusion of explicit provisions in the ITE Law regarding the obligation of electronic system operators to maintain content integrity through mechanisms for time and data integrity verification; (2) the establishment of minimum technical standards in implementing regulations, including cryptographic hash standards (e.g., SHA-256), secure timestamp servers, public

verification mechanisms, and audit log retention; and (3) the implementation of immutable timestamps on podcast platforms as a form of compliance by design.

This proposal does not restrict freedom of expression because it does not filter, censor, or limit content topics. Rather, this policy aims to ensure accountability in the distribution of digital content and legal certainty regarding evidence. From a human rights perspective, the requirement for an immutable timestamp meets the criteria of legitimate aim, Necessity, and Proportionality. Conceptually, the proposed model reflects a shift from *"trust the speaker"* to *"trust the system*," and integrates the approaches *of responsive regulation* and *digital constitutionalism*. In this regard, the government, through the Ministry of Communication and Digital Affairs, needs to regulated podcasters. Thus, the integrity of digital content is no longer merely a forensic issue, but becomes part of the national legal architecture and digital governance. This normative reconstruction is expected to strengthen legal certainty, the efficiency of evidence, and public trust in Indonesia's digital ecosystem.

References

Adnyana, I. M., & Liswahyuningsih, N. L. G. (2025). Pertanggungjawaban Hukum Podcaster di Indonesia: Analisis atas Kekosongan Hukum dalam Penyiaran Digital. *Seminar Nasional Penelitian Dan Pengabdian Kepada Masyarakat*, 117–126. https://ojs.mahadewa.ac.id/index.php/santimas/article/view/5610

Aini, N., & Lubis, F. (2024). Tantangan Pembuktian dalam Kasus Kejahatan Siber. *Judge: Jurnal Hukum*, *05*(02), 55–63. https://doi.org/10.54209/judge.v5i02.566

Aprilianti, A. (2024). Efektivitas dan Implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai Hukum Siber di Indonesia: Tantangan dan Solusi. *Begawan Abioso*, *15*(1), 41–50. https://ejournal.hukumunkris.id/index.php/abioso

Ariyaningsih, S., Andrianto, A. A., Kusuma, A., & Rezi. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia. *Justisia: Jurnal Ilmu Hukum*, *1*(1), 1–11. https://doi.org/10.56457/jjih.v1i1.38

Avianto, L. (2023). *Penguatan Transformasi Digital Media Massa dalam Rangka Ketahanan Nasional*.

http://lib.lemhannas.go.id/public/media/catalog/0010-112300000000168/swf/7684/57 LUCKY AVIANTO.pdf

Baried, R. R. (2022). Penggunaan Alat Bukti Elektronik Dan Problematikanya Dalam Sengketa Perdata di Pengadilan. *Seminar Hukum Aktual: Perkembangan Dan Isu Hukum Keperdataan-Bisnis Kontemporer*, *2*(2), 16–23. https://journal.uii.ac.id/psha/article/view/34024

Casey, E. (2011). Foundations of Digital Forensics. In E. Casey (Ed.), *Digital Evidence and Computer Crime* (Third, pp. 3–32). Elsevier. www.elsevierdirect.com/companions/9780123742681

Cavoukian, A. (2011). *Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices*. www.privacybydesign.ca

Clarke, R. V. (1997). *Situational Crime Prevention: Successful Case Studies* (Second). Harrow and Heston. https://popcenter.asu.edu/sites/g/files/litvpz3631/files/scp2_intro_0_0.pdf

Daeng, Y., Levin, J., Karolina, Prayudha, M. R., Ramadhani, N. P., Noverto, Imanuel, S., & Virgio. (2023). Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia. *Innovative: Journal Of Social Science Research*, *3*(6), 1135–1145. https://j-innovative.org/index.php/Innovative%0AAnalisis

Dewi, S. S., & Suyono, E. (2024). Dampak Teknologi Artificial Intelligent dan Cara Menghadapi Blockchain Technology dalam Perspektif Akuntansi. *Jurnal Ekonomika45*, *12*(1), 975–993. https://univ45sby.ac.id/ejournal/index.php

Dumortier, J., & Vandezande, N. (2012). Trust in the proposed EU regulation on trust services ? *Computer Law & Security Review*, *28*(5), 568–576. https://doi.org/10.1016/j.clsr.2012.07.010

European Commission. (2021). *The EU Digital Identity Framework*. EIDAS. https://eidas.ec.europa.eu/efda/home

Federal Rules of Evidence (2024). https://www.uscourts.gov/forms-rules/current-rules-practice-procedure/federal-rules-evidence

Ferdiyansah, A., Wahyono, B. A. W., Harahap, A., Gustian, E., & Zaidan, D. (2025). Pengaruh Penerapan Undang-Undang ITE Terhadap Tingkat Kejahatan Siber Di Indonesia. *Jurnal Kajian Hukum Dan Kebijakan Publik*, *2*(2), 924–930. https://doi.org/10.62379/bza49768

Grigoras, C. (2005). Digital Audio Recording Analysis: The Electric Network Frequency Criterion. *International Journal of Speech Language and the Law*. https://tracertek.com/media/pdf/an4.pdf

Insa, F. (2007). The Admissibility of Electronic Evidence in Court (A . E . E . C .): Fighting against High-Tech Crime — Results of a European Study. *Journal of Digital Forensic Practice ISSN:*, *1*(4), 285–289. https://doi.org/10.1080/15567280701418049

Kerr, O. S. (2009). Digital evidence and the new criminal procedure. *Columbia Law Review*, *105*(279), 279–318. https://ssrn.com/abstract=594101

Konstitusi, M. (2008). *Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008* (pp. 1–112). Mahkamah Konstitusi. https://www.mkri.id/public/content/persidangan/putusan/putusan_sidang_FINAL PUTUSAN 50 UU ITE 2008.pdf

Lesfandra, Sugiyanto, L., Fairliantina, E., Oktariswan, D., Aries, H., Suprapto, Ananda, Y. P., Mardiana, R., Hidayat, A. Z., & Srietiningsih, P. (2025). Podcast Pengetahuan dan Perlindungan Hak Kekayaan Intelektual di Kalangan Akademisi dan Kreator Muda. *Academica: Jurnal Pengabdian Kepada Masyarakat*, *3*(2). https://doi.org/10.5281/zenodo.16663383

Lessig, L. (2006). *Code: And Other Laws of Cyberspace* (Version 2.). New York: Basic Books. https://lessig.org/images/resources/1999-Code.pdf

Lubis, F., Shabri, I. H., Puspita, S. A., Eprianty, C. N., Rielta, T., & Naim, J. (2025). An Analysis of the Validity of Digital Evidence in the Modern Technological Era. *Fox Justi: Jurnal Ilmu Hukum*, *15*(02), 479–486. https://doi.org/10.58471/justi.v15i02

Lukito, R. (2022). " Compare But Not to Compare ": Kajian Perbandingan Hukum di Indonesia. *Undang: Jurnal Hukum*, *5*(2), 257–291. https://doi.org/10.22437/ujh.5.2.257-291

Marpi, Y., & Sunarno. (2025). Urgensi Ilegal Live Streaming Podcast Melalui Media Youtube dalam Etika Penyiaran. *Yustitiabelen*, *11*(2), 193–208. https://doi.org/10.36563/yustitiabelen.v11i2.1714

Marzuki, P. M. (2015). *Penelitian Hukum* (Edisi Revi). Prenadamedia Group. https://books.google.co.id/books?id=CKZADwAAQBAJ&printsec=copyright#v=onepage&q&f

Menezes, A. J., Oorschot, P. C. Van, & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press. https://theswissbay.ch/pdf/Gentoomen

Library/Cryptography/Handbook of Applied Cryptography - Alfred J. Menezes.pdf

Mueller, C. B., & Kirkpatrick, L. C. (2025). *Federal Evidence* (4th ed., Vol. 103, Issue July 2025). thomsonreuters.com

Mufid, F. L., & Hariandja, T. R. (2019). Efektivitas Pasal 28 Ayat (1) UU ITE tentang Penyebaran Berita Bohong (Hoax). *Jurnal Rechtens*, *8*(2), 179–198. https://doi.org/10.36835/rechtens.v8i2.533

Nahor, T. B., Selan, Y. M., & Hartanto. (2025). Analisis Pertimbangan Hakim Mengenai Pencemaran Nama Baik yang Dilakukan Oleh Tokoh Publik Dengan Putusan Bebas : Studi Putus Nomor 202 / Pid . Sus / 2023 / PN . Jak . Tim. *Jurnal Krisan Law*, *7*(2), 1–9. https://doi.org/10.37893/krisnalaw.v7i2.1068

Nakamoto, S. (2018). Bitcoin : A Peer-to-Peer Electronic Cash System. *2018 National Seminar US Sentencing Commission*, 1–9. https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf

Napoli, P. M. (2019). *Social Media and the Public Interest: Media Regulation in the Disinformation Age*. Columbia University Press. https://lccn.loc.gov/2019021836

Novita, D., Mulyono, & Retnowati, A. (2024). Perkembangan Hukum Siber di Indonesia : Studi Literatur tentang Tantangan dan Solusi Keamanan Nasional. *Innovative: Journal Of Social Science Research*, *4*(6), 1179–1186. https://j-innovative.org/index.php/Innovative%0APerkembangan

Nurullah, A. (2024). Peran Hakim dalam Menilai Keabsahan Alat Bukti Elektronik dalam Perkara Pencemaran Nama Baik. *Celestial Law Journal*, *II*(1), 27–44. https://journal.unsuri.ac.id/index.php/clj/en/article/view/518/341

Pradipa, A. (2025). Analisis terhadap Kedudukan Alat Bukti Elektronik dalam Pembuktian Perkara Perdata Pasca UU ITE dan Perkembangan E-Court. *Konsensus : Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi*, *2*(3), 191–203. https://doi.org/10.62383/konsensus.v2i3.989

Rolph, D. (2025). Truth as a defence : defamation , contempt , confidence , privacy. *Journal of Media Law*, 1–24. https://doi.org/10.1080/17577632.2025.2567732

Sari, I. R., & Rezeki, W. (2025). Podcast peHTem : Inovasi Jurnalisme Digital Alternatif Bagi Masyarakat Informasi. *Insight Journal*, *1*(3), 130–137. https://journal.ynam.or.id/index.php/insight

Sariani, A. L. (2024). Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia. *Al-Dalil*, *2*(2), 69–77. https://ejournal.indrainstitute.id/index.php/al-dalil/index

Seng, D. (2018). *Electronic Evidence* (S. Mason & D. Seng (eds.); Fourth). IALS. http://ials.sas.ac.uk/digital/humanities-digital- library/observing-law-ials-open-book-service-law

Setiawan, A., & Khasanah, U. (2024). Hukum Perdata dan Keamanan Siber: Menanggapi Ancaman dan Risiko Teknologi terhadap Hak-Hak Individu. *JPeHI (Jurnal Penelitian Hukum Indonesia)*, *5*(2), 101–118. https://doi.org/10.61689/jpehi.v5i02.675

Sidabutar, A. C., Priyono, E., Invionita, D. N., Ramadhani, E. O., Maharani, I., Illiyin, J. S., & Raya, J. (2025). Strategi, Etika, dan Inovasi dalam Bisnis Kreatif: Refleksi dari Tayangan Podcast Creativera. *Neraca Manajemen, Ekonomi*, *20*(4). https://doi.org/10.8734/mnmae.v1i2.359

Silaban, A. D., Amirulloh, M., & Rafianti, L. (2020). Podcast: Penyiaran atau Layanan Konten Audio Melalui Internet (Over the Top) Berdasarkan Hukum Positif di Indonesia. *Jurnal Legalitas*, *13*(2), 132–146. https://doi.org/10.33756/jelta.v13i02.8325

Sriwidodo, J. (2019). *Kajian Hukum Pidana Indonesia: Teori dan Praktek*. Kepel Press. https://jdih.banyuwangikab.go.id/dokumen/ebook/KAJIAN HUKUM PIDANA INDONESIA.pdf

Vanessa, V., & Firmansyah, H. (2025). Analysis of the Validity of Electronic Evidence in Criminal Trial Proceedings and the Implementation of Its Admissibility (Judgment Study). *Indonesian Journal of Law and Economics Review*, *20*(4). https://doi.org/10.21070/ijler.v20i4.1395

Widianingrum, A. R. (2024). Analisis Implementasi Kebijakan Hukum terhadap Penanganan Kejahatan Siber di Era Digital. *Journal IURIS SCIENTIA*, *2*(2), 90–102. https://doi.org/10.62263/jis.v2i2.40

Zellatifanny, C. M. (2020). Tren Diseminasi Konten Audio on Demand melalui Podcast : Sebuah Peluang dan Tantangan di Indonesia. *Jurnal Pekommas*, *5*(2), 117–132. https://doi.org/10.30818/jpkm.2020.2050202

Acknowledgments

None.

Declaration of Generative AI Use

During the preparation of this manuscript, the author(s) used Gemini and ChatGPT to support some information, and used DeepL and Grammarly to refine language and improve readability. Following this process, the author(s) critically reviewed, edited, and validated the output to ensure accuracy and scientific integrity. The author(s) maintain full accountability for the final content. AI was used solely as a supportive tool and is not credited with authorship. No the AI performed original data analysis or interpretation without human oversight.

Competing Interest

We declare that the authors have no competing interests regarding the research article.