Priviet Social Sciences Journal
E-ISSN 2798-866X
P-ISSN 2798-6314
https://doi.org/10.55942/pssj.v5i9.558

Volume 5
Issue 9
September Edition 2025

Transhumanistic cybercrime analysis using a posthuman criminology approach to digital identity threats in artificial intelligence era

Tegar Raffi Putra Jumantoro* **& Muhammad Kuttub Firdausy**

Faculty of Law, Jember University, Jl. Kalimantan No. 37, Krajan Timur, Sumbersari, Kec. Sumbersari,
Kabupaten Jember, Jawa Timur 68121
e-mail: tegarraffiputraj@gmail.com

Received 30 July 2025
Revised 27 August 2025
Accepted 31 August 2025

ABSTRACT

The emergence of artificial intelligence has disrupted conventional legal assumptions about identity, subjectivity, and criminal responsibility. This study investigated the normative and systemic inadequacies of Indonesia's legal system in responding to transhumanistic cybercrime, particularly involving the manipulation of digital identities. Employing a normative juridical method and incorporating statutory, conceptual, and comparative approaches, this study critically analyzes structural, substantive, and cultural inertia within the legal framework. Drawing on Lawrence Friedman's legal system theory and post-human criminology, this study identifies a deep ontological crisis wherein non-human actors and synthetic identities remain legally unrecognized. A comparative analysis of the European Union, the United States, Estonia, and Japan illustrates the varying degrees of legal adaptation, from algorithmic accountability to digital identity sovereignty. The findings reveal that Indonesia lacks a coherent legal regime to address algorithm-driven harm or recognize digital identity as an autonomous legal subject. The study proposes legal reforms that include establishing a dedicated legal framework for digital identity protection, extending criminal liability to autonomous systems, and integrating post-human perspectives into legal education. In the age of algorithmic governance, law must transcend biological essentialism to remain legitimate, responsive, and just.

Keywords: post-human criminology, digital identity, algorithmic agency, legal system theory.

1. INTRODUCTION

The presence of Artificial Intelligence (hereinafter referred to as AI) in contemporary digital architecture has created new terrain for transformative cybercrime. Phenomena such as synthetic identity theft, deepfake-based visual engineering, and credential infiltration through algorithmic manipulation are now shaping a criminal landscape that is no longer entirely human (Sarkar & Shukla, 2023). A Cybersecurity Ventures report (2024) estimated that global economic losses from cybercrime reached USD 10.5 trillion in 2025, making it the most systemically destructive form of crime (Otoritas Jasa Keuangan, 2025). Diverging from the classical paradigm that centers human actors as criminal subjects, hybrid entities have now emerged that combine code, algorithms, and human will into a single chain of deviation. Digital identity is no longer simply a data representation but has become a socio-technological construct vulnerable to exploitation through difficult-to-detect reality simulations (Abrar Adhani et al., 2017). This vulnerability is exacerbated by the absence of a theoretical approach capable of explaining the ontological shift in the definition of perpetrators and victims of crime. Therefore, contemporary realities demand a redefinition of the basic postulates of criminology to understand crime in the era of transhumanism.

Empirically, emerging phenomena demonstrate the dominance of cybercrime rooted in identity manipulation, digital representation, and blending humans and machines. Data from the Veridas Identity Fraud Report (2024) indicate that over 80% of identity theft cases in the financial sector involve synthetic elements based on artificial intelligence (Veridas, 2024). Furthermore, a Europol report confirmed that the use of deepfakes for visual and voice manipulation has become a key tool in the escalation of transnational crime, including smuggling, extortion, and political sabotage (Cornelia Riehle, 2022). These developments not only mark technological progress but also indicate a fundamental mutation in the structure of crime itself, where the boundaries between subject and object, and human and machine, are becoming increasingly blurred (Ravizki & Lintang Yudhantaka, 2022). This phenomenon represents das sein, a factual condition in which conventional legal and criminological systems have proven stagnant and are unable to anticipate the logic of contemporary criminality. The absence of a conceptual framework capable of understanding the ontological relationship between digital identity and criminogenicity in the post-human realm is a pressing issue (Agustin, 2019). Therefore, theoretical intervention is not merely a methodological choice, but an epistemological imperative.

Instead, das Sollen demands a conceptual formulation capable of navigating the post-structural and transhuman dimensions of criminology. Posthuman criminology, as a marginal theoretical branch, offers analytical tools to challenge the anthropocentrism of classical criminology. This framework shifts the orientation from a human subject to a network of biological and artificial entities that collectively form a criminal ecosystem (Osborne & Rose, 2024). Amidst accelerating digitalization and automation, post-human criminology enables the remapping of the perpetrator entity, algorithmic power structures, and the distribution of social vulnerability arising from the relationship between humans and machines (Gilani, 2021). This perspective also opens up a new ethical discourse on who is responsible for criminal acts in spaces inhabited by autonomous systems. As a normative approach, post-human criminology offers a new foundation for reformulating digital identity governance policies that are more reflective of the complexities of the times. Thus, the moral and legal imperative going forward is to create a system that recognizes the existence of posthuman entities as relevant legal subjects (Mark Taylor & Mireille Meissner, 2019).

Previous studies have not significantly synthesized the threat of digital identity and post-human theoretical approaches. First, Sandoval de Almeida Vau et al. (2024) only emphasized the technical and institutional aspects of the deepfake threat to the criminal justice system, without elaborating on the epistemological and ontological dimensions of digital identity manipulation within the framework of posthumanistic crime (Sandoval et al., 2024). Second, the study by Haggerty and Trottier (2020) proposed a critical perspective on digital surveillance through network analysis and self-representation, but did not link it to the construction of digital identity as a legal subject within the framework of post-human criminology. Thus, there is an epistemological lacuna in the form of the absence of a theoretical framework capable of bridging the complexities between digital identity, transhumanism, and criminal practices

(Kevin D. Haggerty & Daniel Trottier, 2015). his gap is important to fill, not only for academic purposes, but as a response to the crisis of representation and identity regulation in the global digital order. An interdisciplinary approach combining critical theory, the philosophy of technology, and criminology is necessary to produce new transformative knowledge. Therefore, this study aims to break through intellectual stagnation and present an alternative discourse on the dynamics of contemporary crime.

This research offers conceptual novelty by combining transhumanistic cybercrime and post-human criminology as an analytical framework for the digital identity crisis. On the one hand, the concept of transhumanistic cybercrime is intended to capture the reality of crimes committed by and through hybrid entities, the result of the interfusion of humans and artificial intelligence (Tabiu et al., 2023). On the other hand, posthuman criminology provides a reflective space for understanding structures of domination and subordination that no longer occur between humans but also involve non-human agents (Zul Khaidir Kadir, 2025). Methodological uniqueness is also evident in the semi-critical approach to the construction of digital identity as an arena for the contestation of algorithmic power. By highlighting empirical cases from across jurisdictions, this study also contributes to building a global policy framework that is more adaptive to post-digital reality. Therefore, this research not only broadens the horizons of critical criminology, but also challenges the ontological boundaries of understanding criminality. This novelty makes this research a relevant and urgent theoretical intervention amidst the global identity governance crisis.

Specifically, this study aims to investigate the structural transformation of cybercrime rooted in the disruption of artificial intelligence to the construction of digital identity in a post-digital society. This research focuses on (1) examining the limitations of positive law in addressing the dynamics of AI-based digital identity crime, (2) exploring the theoretical dimensions of non-human agency as a criminogenic entity in virtual social structures, and (3) examining cross-jurisdictional regulatory practices to identify adaptive and contextually translatable normative patterns. This study also presents a conceptual critique of the stagnation of conventional criminology, which has not yet anticipated an ontological shift from legal subjects to hybrid entities. From an applied perspective, this study aims to develop a recommendatory framework for national and international policymakers in response to the crisis of legal legitimacy regarding digital identity. Its theoretical contribution lies in expanding the horizons of critical criminology through the integration of post-human perspectives, which have been marginalized in cyber law discourse. Thus, this research not only presents a descriptive analysis, but also builds a normative foundation for a more reflective and futuristic legal transformation.

The benefits of this study are multilevel and cross-sectoral. At the academic level, this research broadens the theoretical horizons in criminology studies by integrating post-human epistemology into the analysis of digital crime. In the policy realm, research findings can be used to formulate new regulatory tools for digital identity verification, track the activities of hybrid entities, and mitigate transhuman crimes. Technological benefits arise from the potential application of trustless system-based identity models, such as digital identity wallets that are compatible with post-human contexts (Ansaroudi et al., 2023). For a wider community, this research increases literacy regarding understudied forms of digital crime, particularly in the context of deepfakes and algorithmic intrusions. Globally, this research contributes to building a collective narrative regarding the protection of digital rights in the post-human era. Furthermore, this study has the potential to spark new legal and criminal approaches that are more responsive to the complexities of contemporary identity and crimes. Thus, the benefits of this research are not only academic, but also structural and cultural.

2. METHODOLOGY

This study uses the normative juridical method as the main approach, namely, a type of legal research that relies on the analysis of applicable written legal norms, both in statutory regulations, legal doctrines, and legal principles that have developed theoretically and practically. This method is relevant for studying the phenomenon of digital identity crime in the context of artificial intelligence, which has not been fully accommodated by the applicable positive legal system. In this research, three approaches are used: first, the statute approach, which is used to examine normative provisions in national laws and regulations such as the Electronic Information and Transactions Law (UU ITE), the Personal Data Protection Law, and relevant international legal instruments; second, the conceptual approach to explore and dissect contemporary legal and criminological theories, especially the theory of post-human criminology as an interpretative basis for the reality of digital crime that is transhumanistic in nature; and third, a comparative approach, to examine legal policies and practices developing in various international jurisdictions, such as the European Union, the United States, and Estonia, which are considered more progressive in responding to threats to AI-based digital identity (Endang Purwaningsih, 2022).

Data collection techniques were conducted through literature review, exploring primary legal materials in the form of laws and regulations, international conventions, and relevant court decisions, and secondary legal materials in the form of books, scientific journals, research reports, policy documents, and academic publications from various disciplines of law, criminology, and information technology. Tertiary legal materials such as legal encyclopedias, legal dictionaries, and bibliographic indexes were also used to support conceptual understanding (Nitaria Angkasa, 2019). All data were analyzed qualitatively using prescriptive and descriptive-analytical methods, namely, systematically examining legal provisions and then constructing normative solutions to the identified problems. To maintain the validity and credibility of the interpretation, data triangulation techniques were used through a cross-comparison between positive regulations, academic theory, and international legal practices (Zuchri Abdussamad, 2021). Thus, the results of this study are expected to reflect not only normative rigor but also analytical accuracy in addressing the complexity of digital crime in the post-human realm, which transcends conventional legal boundaries.

3. RESULT AND DISCUSSION

3.1. Legal Restrictions in Regulating Digital Identity and Transhumanistic Cybercrime in the National Legal System

The transformation of human identity into digital form is no longer merely a technological consequence but rather a legal mutation that demands a re-articulation of the normative boundaries of the existence of legal subjects. In the Indonesian context, the positive legal system is not yet fully prepared to accommodate this complexity, especially as digital entities have begun to play an active role in social and economic dynamics. The emergence of artificial intelligence capable of creating false identities based on synthetic data, deepfakes, and auto-generative profiles creates a legal vacuum that has the potential to become a crisis point (Adnasohn Aqilla Respati, 2024). When individuals are reduced to data, and data are manipulated by non-human entities, the pressing question is: is the law capable of adequately recognizing, protecting, and prosecuting deviations from this digital identity? The lack of a legal definition of "digital identity" in national legislation emphasizes the urgency of critical reflection on the still-conventional legal approach (Kadek Ayu Widya Arisanthi, 2025). Legal articulation of post-human entities remains very limited, even tending to ignore socio-technical realities that have exceeded their regulatory capacity.

In general, regulations related to digital crime in the Indonesian legal system still rely on Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which has been revised several times, most recently through Law Number 1 of 2024. However, the norms in the ITE Law only define and formulate criminal acts based on illegal access and data manipulation without distinguishing between human subjects and artificial digital entities (Jaya & Goh, 2021). Articles regarding crimes against data integrity, the distribution of illegal content, and defamation do not cover actions based on generative algorithms or biometric manipulation. Thus, the ITE Law operates within an instrumental paradigm rather than a deeper ontological relationship between identity, personality, and machines. When an AI system replicates a person's identity in real time for fraudulent purposes, existing regulations are insufficient to confirm whether the perpetrator is the programmer, user, or system itself (Mawlidy et al., 2024). Criminal law still requires the existence of humans as a single reference point, even though transhumanistic crimes are distributed and cannot always be traced to biological actors. Therefore, the legal space for non-traditional forms of accountability has not yet been adequately provided in the national positive law.

Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) was introduced in response to global demands for privacy, but it still treats personal data within an administrative, rather than criminal, framework. The PDP Law regulates the position of data subjects as information owners and establishes obligations for data controllers but does not provide criminal provisions for entities or systems that autonomously manipulate identities (Fauzi & Radika Shandy, 2022). Even in the administrative realm, an agency is always assumed to lie with human legal entities or corporations. This creates a serious gap when violations are committed by machine-learning-based systems that operate independently through data mining and cross-platform aggregation (Cecez-Kecmanovic, 2025). Therefore, it can be argued that the PDP Law contains a normative gap in terms of protecting synthetic identity construction and forms of identity generated by AI rather than by human individuals. Furthermore, the absence of a clause on recognizing digital identity as a "legal entity" results in a lack of basis for establishing limits on responsibility and legal rights regarding the manipulation of non-biological forms of identity (Campione, 2025). This further reinforces the assumption that national law lacks a modern conception of identity as a virtual entity living within the digital ecosystem.

Overlapping regulations also pose significant obstacles to law enforcement. Despite overlapping areas, the ITE Law and the PDP Law have not been systematically harmonized, leading to uncertainty in implementation. For example, violations of identity data in the form of biometric forgery are subject to sanctions under both but with different evidentiary and processing regimes (one criminal and one administrative) (Mahameru et al., 2023). In practice, law enforcement officials face a dilemma in determining the most appropriate legal framework, especially in the context of perpetrators operating across borders or systems that are not bound by national jurisdiction. Often, the law enforcement process stagnates due to procedural dualism; the violation should be handled as a criminal offense or an administrative violation that can be resolved through fines or warnings. This demonstrates that harmonization between existing regulations has not been effective, and instead creates loopholes for digital criminals to exploit the blurring of normative jurisdictional boundaries.

From an implementation perspective, significant obstacles also arise from the limited technical and institutional capacities of law enforcement institutions. Investigators and prosecutors are not equipped with adequate digital skills to trace, verify, and reconstruct hybrid, dynamic, and non-physical forms of digital identity (Muhammad Singgih Imam Wibowo et al., 2024). No digital identity forensic agency is capable of identifying algorithmic manipulation or AI-based forgery in real time. Consequently, in many cases, evidence fails to meet the "beyond reasonable doubt" standard required by criminal law (Nimerodi Gulo & Cornelius Dikae Zolohefona Gulo, 2024). Meanwhile, criminals are becoming increasingly sophisticated in their use of encryption methods, decentralized networks, and anonymization services, making digital tracing nearly impossible without the support of a robust national cyber structure. Therefore, it can be said that the enforcement gap is not only structural, but also cultural, as the legal system still views digital reality as an accessory, not a primary arena. This results in courts frequently failing to adjudicate AI-based cases because evidence, procedures, and substantive understanding are not readily available within existing procedural law (Beryl Helga Fredella Hibatulloh, 2025).

The issue of digital identity is inextricably linked to the structure of legal accountability, which presupposes human agency as the sole legal subject. However, in today's digital ecosystem, the human role in crimes is often limited to the initial trigger, whereas the operational process is carried out by a system that operates autonomously. This is where national criminal law demonstrates its backwardness in addressing the phenomenon of distributed agency, in which perpetrators are not isolated but distributed across a network of devices, data, and algorithms. When fake identities are created, used, and modified without direct human intervention, the logic of classical accountability is irrelevant. In this case, the lack of a legal basis that allows for collective, vicarious, or even strict liability for non-human entities creates a gap that urgently needs to be filled (Dwi Kurniawan & Indri Hapsari, 2022). Without this broadening of normative horizons, national legal systems will never be prepared to face the phenomenon of criminality that operates entirely in the post-human space.

The legal crisis of digital identity recognition is also evident in the limitations of national doctrine and jurisprudence. To date, no single court decision in Indonesia declares digital identity to have intrinsic value, capable of being owned, transferred, or protected on par with other civil rights. Digital identity is still considered a derivative of civil identity, despite the fact that in many cases, individuals lose access to financial and social services, even their social existence, due to digital identity manipulation that does not directly impact biological identity (Kadir, 2025). In this context, jurisprudential vacuum reflects the absence of a progressive legal interpretation capable of addressing today's digital challenges. Without a progressive legal precedent, the space for reform will continue to be hampered by legal conservatism, which only dares to operate within an analog framework. Therefore, the development of legal arguments regarding the recognition of digital identity as a constitutional right worthy of guarantee must be carried out immediately in various legislative and judicial forums.

The evidentiary aspect of criminal procedure law also faces significant challenges in AI-based digital identity crimes. The Criminal Procedure Code (KUHAP) and its derivative normative instruments do not yet have relevant evidentiary standards to identify "actions" committed by algorithmic systems. Furthermore, existing digital forensics still focus on tracing human activity (logs and metadata) rather than reading the intentionality of automated systems (Gemilang, 2025). However, understanding deepfake, synthetic identity, or auto-generated impersonation crimes requires evidentiary instruments that detect the technological process and not just the end result (Patricia Morisa Banfatin et al., 2024). Thus, a procedural vacuum exists in procedural law that has not yet been developed to meet the challenges of crimes in the AI era. This exacerbates the gap between technological realities and legal systems that are based on physical and visual principles. Without redesigning evidentiary mechanisms, the criminal justice system will always lag the pace of criminal technology.

Other legal issues also arise in the context of cross-border jurisdiction and enforcement, particularly because the majority of digital identity violations occur within global networks that recognize no territorial boundaries. Indonesia does not yet have a mutual legal assistance (MLA) agreement specifically addressing digital identity crime or data exchange with countries that source or host the crime (Alghazali & Siagian, 2024). The ASEAN cooperation framework for cybercrime is still in its initial stages and has not yet addressed the technical substance of digital identity protection (Putri, 2021). Without a strong transnational legal regime, Indonesia will remain a consumer of regulations and will not effectively protect its citizens in the global digital realm. Therefore, legal reform must incorporate an international dimension to ensure that legal efforts are not cut off by national geographic boundaries, which have long been illusory in the digital context. Therefore, synchronization between national law and international mechanisms is an integral part of a structural solution to the transnational digital identity crisis.

Overall, Indonesia's positive legal framework for responding to AI-based digital identity crimes exhibits various forms of normative lag, overlapping substances, and obstacles to implementation on the ground. The lack of a legal definition for digital identity, unregulated non-human agency, weak technical capacity of institutions, and lack of integration of sectoral regulations indicate that national law is unable to address today's transhuman and non-linear reality. These limitations cannot be overcome with partial revisions or the addition of articles; rather, they demand an epistemic overhaul of how the law interprets identity, agency, and responsibility. Legal reform in this context is not only about norms but also about paradigms and institutions. Therefore, the legal reconstruction of Indonesia's positive legal structure must be systemic, cross-sectoral, and forward looking. Otherwise, the Indonesian legal system will continue to lag, not only technically but also philosophically, in addressing the challenges of future digital crime.

3.2. Systemic Disintegration of Law in Addressing Transhumanistic Crime Through a Theoretical Interpretation of the Digital Identity Crisis

Contemporary legal systems face a fundamental anomaly when confronting transhumanistic crimes that no longer rely solely on human agency. From Lawrence Friedman's legal system perspective, the legal system consists of three main elements–structure, substance, and legal culture–which must work coherently to ensure normative effectiveness (Al Kautsar & Muhammad, 2022). When crimes are committed by or through non-human entities such as artificial intelligence, all three experience simultaneous disruptions. Legal institutional structures are not constructed to respond to algorithmic entities such as perpetrators or instigators of unlawful acts. The substance of law remains grounded in classical conceptions of identity and responsibility that center on humans as legitimate legal subjects. Meanwhile, legal culture remains permeated by normative positivism, which refuses to acknowledge the relationship between law and the fluid and adaptive realities of technology. In such a system, the law not only loses its capacity to act but also its ontological relevance. Therefore, it is no exaggeration to say that transhumanistic crime reveals latent disintegration within the modern legal system.

Posthuman criminology, as a conceptual framework, rejects the conventional view that monopolizes the meaning of criminality solely in humans. In this school, agency is seen as a dynamic distribution between humans, machines, data, and the technological environment, where criminal acts are the result of complex relationships, not simply individual moral wills. Digital identity crimes, for example, do not always stem from human malice but can arise from the architecture of digital systems that automatically generalize or replicate identities (King et al., 2020). In such a logic, perpetrators can no longer be singled out, and the structure of intention (mens rea) is obscured. Therefore, a legal approach that recognizes only humans as actors and actions as a result of will become outdated and unable to address new forms of crime. Bruno Latour's theory of non-human agency reinforces this position, asserting that technological objects and systems also play a causal role in social and legal events (Robertus Robet & U Abdul Rozak R, 2023). Laws that fail to recognize digital entities as participants in action networks ignore the reality that today's technology functions autonomously and adaptively. Consequently, justice is not achieved because perpetrators remain unidentified and victims are unprotected.

The digital identity crisis in the legal sphere can be interpreted as the failure of the legal system to respond to ontological changes in social structures. Identity is no longer solely tied to the biological body but is constructed through data, biometrics, algorithms, and digital recognition. In many cases, these new forms of identity lack legitimate legal representation in a legal system based on civil documents and residency status (Sih Yuliana Wahyuningtyas et al., 2025). This creates a gray area where individuals can be digitally attacked, misrepresented, or reconstructed without the legal recognition of their digitally owned entities. This vacuum creates a space of impunity where crimes against identity cannot be prosecuted because the victims are not recognized. Friedman's model emphasizes the importance of legal substance that reflects social reality, but in Indonesia, the legal substance has not substantively addressed the problems of digital identity. The concept of "who" constitutes a legal subject still relies on a manual population system, which fails to address AI-based identity. Therefore, the Indonesian legal system has been ontologically stagnant (see Figure 1).

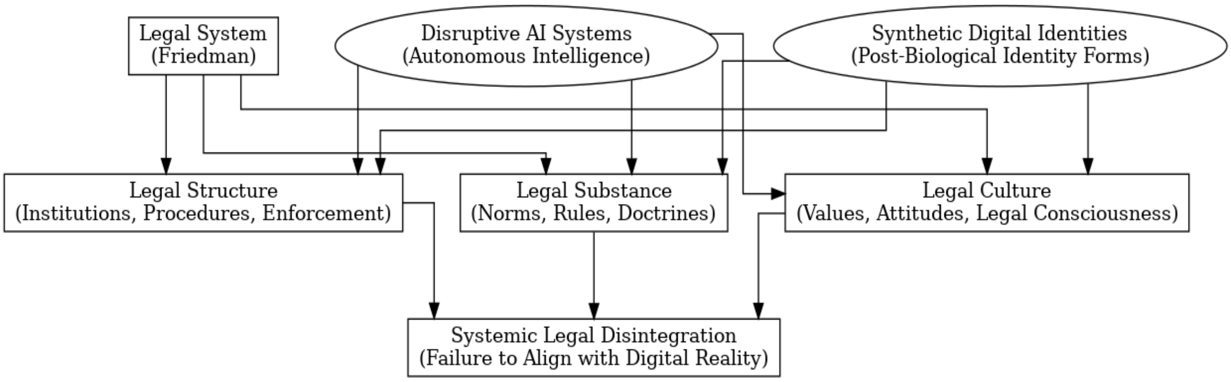
Legal System
(Friedman)
Disruptive AI Systems
(Autonomous Intelligence)
Synthetic Digital Identities
(Post-Biological Identity Forms)
Legal Structure
(Institutions, Procedures, Enforcement)
Legal Substance
(Norms, Rules, Doctrines)
Legal Culture
(Values, Attitudes, Legal Consciousness)
Systemic Legal Disintegration
(Failure to Align with Digital Reality)

Figure 1. Mapping Legal System Failure in the Digital Age Using Friedman's Framework
Source: Author, edited

From a legal perspective, law enforcement agencies lack the technical and methodological tools to handle digital crimes based on synthetic identities. The lack of a digital identity forensic authority or unit means that many cases of data manipulation or profile manipulation never reach the judicial system (Cahyono et al., 2025). On the one hand, Indonesian criminal procedure law does not yet provide a mechanism to verify virtual identities as authentic evidence (Aini & Lubis, 2024). On the other hand, law enforcement officials often lack an understanding of the characteristics of AI, which can operate autonomously, nonlinearly, and impersonally. Therefore, the legal structure is not only underdeveloped in terms of infrastructure but also in terms of epistemology. Friedman stated that a legal system that fails to build a structure compatible with reality will create systemic friction that accelerates legal delegitimization. In this regard, the Indonesian legal system lacks a responsive structure that can accommodate the dynamics of AI-based digital crimes. This underscores that dysfunction is not merely technical but also systemic.

Legal culture, one of the pillars of Friedman's system, plays a central role in determining the pace and direction of legal change. However, in the reality of Indonesian law, legal culture remains highly conservative in accepting post-human entities as legally meaningful entities. The dominance of positivistic and legalistic approaches has resulted in legal interpretations that are limited to the textual level rather than addressing the empirical problems emerging in digital society. As a result, despite the urgency of protecting digital identities, the drive of legal culture to normalize digital entities as legal subjects remains low. Public discourse on digital identity is often interpreted in administrative or technical terms rather than as a substantive legal problem affecting citizens' fundamental rights (Danrivanto Budhijanto, 2025). Furthermore, lawmakers still rely on analogies with existing laws rather than developing new legal concepts. This non-adaptive legal culture constitutes an epistemological obstacle exacerbating the dysfunction of substances and structures. In other words, without a legal cultural revolution, digital law reform will be merely a cosmetic revision.

The theory of legal fiction proposed by Hans Kelsen can open up conceptual space for the recognition of digital entities as legitimate legal subjects (Ida Bagus Wisnuputra Raditya & I Dewa Gede Dana Sugama, 2024). Within this framework, empirical existence is not necessary for granting legal status to a particular entity; rather, a normatively valid legal construction is sufficient. This means that digital identities, despite their intangible nature, can be fictionalized as legal entities with rights and obligations. However, the Indonesian legal system has not progressively developed this doctrine, and still relies on the principle of physical document-based identification. This complicates the process of protecting victims of digital crime who lose control of their identities despite the real impact of the harm. By adopting a legal fiction approach, law can transcend biological limitations in determining who is entitled to protection or punishment. This is a crucial step in integrating post-human realities into the national legal framework. However, moving in this direction requires legal political courage and radical epistemological commitments.

Luhmann's social systems theory states that law is an autonomous system that can only adapt through internal mechanisms (autopoiesis) (Constantin & Sitorus, 2024). Within this framework, the legal system must be able to create new codes and mechanisms that align with the complexity of digital society. If the legal system continues to reproduce old norms without adapting to network and algorithmic logic, it will become a closed system and lose its communicative functions. Digital identity crimes committed by AI systems will never be legible if the law relies on the logic of the physical relationship between perpetrators and victims. Therefore, the law must create new communication codes to address the layers of reality that are now nonlinear, adaptive, and multi-entity. Legal autopoiesis means that the legal system must not wait for external realities but must be able to carry out semantic and structural transformations from within (Aal, 2022). In this regard, transhumanistic crimes must be addressed not simply by adding new articles, but by dismantling and redesigning the legal paradigm. Without this, the law would simply be a system that rewrites the past and does not design the future.

One of the fundamental failures of the legal system in responding to transhumanistic crime is its inability to create a new normative framework that recognizes the existence of non-human forms of agency. Amid the digital revolution, where artificial intelligence plays a role not only as a tool but also as a subject in the criminal ecosystem, the legal system remains constrained by the concept of the perpetrator-criminal relationship rooted in the classical legal paradigm. In many cases, digital identity-based crimes cannot be prosecuted simply because the law cannot recognize the relational structure between humans and technological systems as a complex structure of intentions and actions. Yet, in posthuman logic, AI is no longer a passive instrument but an active element that shapes decisions, predictions, and criminal actions autonomously and repeatedly. Friedman, in his conception, emphasizes that law must evolve from an ever-changing social life, and that the substance of law must be able to absorb the social dynamics that occur. If the legal structure and culture do not support the renewal of substance, the system will fail to regenerate internally. In this regard, transhumanistic crime is clear evidence that the law is not only lagging behind, but also frozen in old, inoperative categories. Therefore, a legal approach that continues to uphold the subject-object and human-nonhuman dichotomies constitutes an untenable form of epistemic regression.

Furthermore, the national legal system has not yet developed a new legal accountability mechanism to autonomously operate digital entities. In the Indonesian criminal system, criminal liability always presupposes the conscious and rational intent or negligence of human subjects. However, in AI-based digital identity crimes, intent is no longer a classically tractable category because the system can "learn" from data and make its own decisions based on its code architecture. Therefore, a renewed legal accountability doctrine is needed, based not only on individual culpability, but also on structural, systemic, or even algorithmic responsibility. Several legal systems around the world have begun to introduce the concept of "electronic legal person" or "autonomous system liability," but in the Indonesian context, this discourse has not yet developed seriously (Puspita Sari & Harwika, 2022). This lag indicates that the Indonesian legal system has not yet entered the epistemological transition phase necessary to understand post-human agency as a normative subject. Friedman argued that the failure of legal substance to evolve according to societal needs will result in the law losing its function as a means of control and resolution of conflict. In this regard, legal reform to address transhumanistic criminality must begin with comprehensive deconstruction and reconstruction of the theory of legal responsibility.

Furthermore, the legal system has yet to provide a normative basis for protecting digital identity as an autonomous legal right independent of biological identity. Within the contemporary human rights framework, identity has shifted from a static concept to a dynamic, fluid, and multidimensional entity, represented not only through the physical body, but also through data representation in digital systems (Anggen Suari & Sarjana, 2023). In many countries, the right to digital identity is beginning to be recognized as part of the right to personality and privacy that must be legally protected. However, in Indonesia, regulations still treat personal data as administrative information and not as an existential element that legally shapes a citizen's identity. The absence of a legal concept that views digital identity as a constitutional right makes violations of it considered minor or merely technical matters, even though its impact can be very destructive socially, economically, and psychologically. In Friedman's view, when the substance of the law fails to capture the social values that have developed in society, tensions arise between formal law and living law. As a result, the legal system will become increasingly distant from the society it serves and lose its legitimacy as a normative institution. Therefore, updating the concept of digital identity rights and protection is not merely a technical necessity, but also a normative necessity to reaffirm the essence of law as a protector of humans and their existence, both physical and digital.

The implication of all this is the urgent need to redesign the legislative roadmap and criminal justice system to face post-human challenges. Legislation can no longer be formulated with linear logic that treats technology as an external variable; instead, it must integrate artificial intelligence as an inherent part of the legal and social landscape. Friedman's approach provides an important lesson: laws that fail to transform with societal changes will be left behind and ultimately abandoned. Therefore, legal reform requires not only changes in norms, but also shifts in orientation, institutional structures, and the mindset of legal culture. This means that legal education must adopt a curriculum that integrates an understanding of AI, digital identity, and post-human ethics as part of the formation of future legal professionals. Furthermore, the justice system must establish specialized units to handle digital crime cases from the perspective of transcending conventional legalism. This transformation is not only crucial for the sustainability of national law but also an absolute requirement for law to remain an instrument of justice amidst an increasingly hybrid reality. If the law fails to undergo this process, it will not only become irrelevant but also become an obstacle to justice.

The digital identity crisis mediated by artificial intelligence systems is not simply a new criminal challenge but also an epistemological challenge for the law to redefine itself. In a world dominated by digital representation and automated actions, law cannot survive the old paradigm that limits legal subjects to biological bodies and conscious intentions. The Indonesian legal system must be willing to enter a phase of radical renewal, in which the law not only adapts but also redesigns the fundamental conceptions of perpetrators, victims, and unlawful acts. Friedman's theory of the interdependence of legal structure, substance, and culture provides a reflective framework for evaluating the current failures of the law and how to initiate change. Addressing transhumanistic criminality can no longer be postponed, as any delay allows citizens' identities to continue to be threatened in a space no longer regulated by law (Wendy et al., 2021). Therefore, the agenda of legislation, doctrinal renewal, and institutional transformation must begin with the courage to acknowledge that the world has changed and the law must change with it. Without it, the law will become nothing more than an artifact of the past in a society already living in the future. It is time for law to stop defending the old reality and begin serving the new existence of humans, who now live as data.

3.3. Convergence and Divergence of Legal Regimes in Addressing Transhumanistic Digital Identity Crimes in the Postbiological Era

Digital identity crimes rooted in the agency of technological systems challenge the anthropocentric foundations of national and international laws. Across the global landscape, various jurisdictions have responded to this phenomenon with different approaches across substantive, institutional, and paradigmatic dimensions. A comparative legal approach in this context is crucial not only for imitation but also for analyzing the epistemological logic underlying the formation of legal norms and practices in other countries. The phenomenon of transhumanistic crime cannot be approached with a purely legalistic narrative, but requires a comprehensive understanding of how digital identity is formulated, recognized, and protected within specific legal systems. Countries such as Estonia, the European Union, the United States, and Japan have initiated legal reforms that are not only technocratic, but also normative-ontological, shifting the boundaries between biological and digital entities. This comparative study explores not only the successes, but also the dilemmas and legal gaps that arise from the complexity of non-human agency. In this context, Indonesia lags behind, but has the opportunity to leapfrog by designing a more reflective digital legal framework based on post-human principles. Therefore, this comparative reading serves as an instrument for articulating non-negotiable legal transformations in addressing AI-based cybercrime.

In Europe, the European Union has adopted the General Data Protection Regulation (GDPR), a milestone in protecting digital identities and personal data. The GDPR not only creates a regulatory regime for corporate entities and digital platforms, but also recognizes citizens' autonomous rights over their data and digital identities (Sirait, 2019). Although the GDPR does not explicitly regulate non-human agents as legal subjects, its protection mechanisms provide space for a post-human reading of digital identities as legal entities worthy of protection. In contrast, the United States relies more on a sector-based and contractual approach, with protections scattered across various laws, such as the California Consumer Privacy Act (CCPA) and the Computer Fraud and Abuse Act (Li, 2019). Estonia has taken a radical path by digitizing its entire state system through residency and the Digital Nation concept, which grants administrative and legal rights to digital identity entities and even to non-citizens (Luhur et al., 2025). Japan, on the other hand, has begun developing a legal framework for recognizing autonomous digital entities in the industrial sphere, with an approach that accommodates AI in contracts and product liability (Ricciardi Celsi & Zomaya, 2025). This comparison demonstrates that legal reform must be not only responsive but also imaginative towards entities that were previously not considered legal subjects. Table 1 compares the legal frameworks of the four major jurisdictions.

Table 1. Legal Comparison of Digital Identity Protection Across Jurisdictions

Jurisdiction	Regulation	Digital Legal Subject	Approach	Distinctive Feature
European Union	GDPR (2016)	Users as data owners	Rights-based	Data ownership and right to digital identity erasure
United States	CCPA, CFAA, sectoral privacy laws	Digital contractual entities	Market-driven	Limited protection depending on jurisdiction and economic sector
Estonia	e-Governance Act, e-Residency program	Administrative digital identity	State-integrated	Fully digitalized state with global participation
Japan	AI Governance Principles, Metaverse Policy Frameworks	Autonomous entities in industry	Techno-regulatory	Function-based protection and AI liability frameworks

Source: Author, edited

This comparison demonstrates that no legal system explicitly affirms nonhuman agency as a full legal subject. However, the global trend is toward normalizing the role of digital entities in the legal sphere through specific rights, obligations, or regulations. In this regard, Indonesia lacks a comparable legal framework, either substantively or institutionally. The ITE Law and PDP Law still operate at the level of administrative protection, failing to address the ontological dimension of digital identity as an integral element of personality. When algorithms can create, duplicate, or steal digital identities, identity protection can no longer be interpreted as protection of "data," but rather as protection of existence (Fajar et al., 2023). This comparison reveals that digital identity protection must be interpreted across a spectrum of recognizing identity as a human right, an administrative function, and an economic object. Therefore, Indonesia requires a paradigm shift from protecting data as an object to recognizing identity as a posthumanistic legal subject.

The concept of "digital identity" in countries like Estonia is no longer viewed as an administrative extension of biological identity, but rather as an independent entity with the legal capacity to act within the legal sphere of the state. This approach allows individuals to participate in legal, economic, and political systems without a physical presence, disrupting the classical concepts of citizenship, jurisdiction, and legal accountability. Meanwhile, the European Union provides individual protection by expanding the concept of "self" to encompass data, algorithms, and digital footprints. In this approach, digital identity crimes are viewed as violations of existential rights that are both integral and transbiological. By contrast, the Indonesian legal system remains trapped in the concept of identity as an administrative attribute proven through a National Identity Card (KTP), Taxpayer Identification Number (NPWP), or passport. Consequently, crimes that attack digital constructs are not treated as identity violations (Rahmawati et al., 2025). Consequently, many cases of profile falsification, digital impersonation, and AI-based entity duplication have not received serious attention from law enforcement. Therefore, this comparison reflects the need to shift the concept of identity-in-law from the administrative realm to the ontological realm, addressing the core of contemporary human subjectivity.

In the context of accountability, the Japanese legal approach is beginning to provide space for constructing responsibility for artificial intelligence systems that cause harm or violate law. This suggests that legal systems can gradually develop new liability mechanisms based on algorithmic function, potential harm, and design, rather than waiting for a positive legal definition of “non-human actors.” In Indonesia, this gap has created a situation of systemic impunity for AI-based criminal acts owing to the lack of a normative basis linking responsibility to non-physical entities. In this context, legal systems should learn from the principles of strict liability in environmental law or product liability in consumer law, which can serve as a bridge to algorithmic liability (Praja et al., 2016). This comparison demonstrates that legal transformation does not require major legislative breakthroughs but can begin with adjustments to the interpretation and precedents of existing doctrines. Articulating legal responsibility in a post-human world does not mean surrendering the law to machines, but rather restructuring the law to capture distributed, collective, and less tangible forms of responsibility. Therefore, the Japanese approach can be adopted as a starting point for developing a legal responsibility framework in Indonesia to deal with autonomous digital entities.

This comparison also reveals that the success of legal reform is determined not only by the text of the law but also by the institutional ecosystem and legal culture that supports it. Estonia, for example, succeeded in establishing a digital regime not only because it had progressive laws but also because of a comprehensive digital infrastructure system, ongoing training of law enforcement officers, and public acceptance of changing identity paradigms (Firman, 2018). Meanwhile, in Indonesia, the biggest challenge is not simply the absence of norms, but the resistance of institutions and legal culture to epistemological changes that challenge the established authority. Therefore, adapting to international developments does not simply mean importing norms but rather undertaking institutional transformation that allows the law to thrive in digital reality. Without this, comparative law simply serves as a showcase for norms that are dysfunctional in the domestic context. This comparison demonstrates that Indonesia needs to design its own digital legal model based on the principles of justice, security, and recognition of digital existence as part of constitutional rights. Therefore, a comparative legal approach should be read as a tool for reflection rather than duplication.

A comparative approach opens up opportunities for the paradigmatic reconstruction of national law to address transhumanistic crimes. No single legal system has perfectly addressed the complexities of AI-based digital identity crimes, but directions and principles can be adapted and adjusted. Indonesia could develop a hybrid model that balances rights protection, accountability, and sustainability. Cybercrime can no longer be combined with conventional legal approaches that rely on humans as sole legal actors. Therefore, courage is needed to affirm posthuman as a legitimate area within the construction of law and human rights. Using a reflective, transformative, and conceptual approach, Indonesian law can become a pioneer in developing a digital legal regime based on transhumanistic justice. It is time for Indonesian law to stop relying on the metaphysics of the body and begin to defend its digital existence as part of the legal subject of the future. To do so, there is no other way to dismantle and rebuild our legal landscape from its fundamental foundations.

4. CONCLUSIONS

This research has uncovered the deepest layers of dissonance between the modern legal system and an increasingly post-human and transbiological criminogenic reality. The ontological changes in identity, legal subjects, and criminal agencies resulting from the penetration of artificial intelligence can no longer be addressed within a reactive, procedural, and anthropocentric normative framework. Digital identity has detached from the biological body and has emerged as a new locus of existence requiring legal recognition as an entity with status and rights. In such circumstances, the legal system cannot simply fix technical details or revise administrative clauses; it must undergo profound deconstruction of the paradigmatic foundations that have limited the space of justice to the human body. If law is to survive as a valid language of legitimacy in a digital society, it must develop new structures of responsibility, affirm the plurality of legal subjects, and expand the horizon of protection into non-physical dimensions of human existence. Normative articulation of the digital world is inseparable from the value struggle over who deserves recognition, protection, and prosecution. In this regard, courage to dismantle the legal system from within is a prerequisite for the birth of justice in the increasingly dominant algorithmic era. Therefore, legal reform regarding transhumanistic crimes is not merely a response to disruption but a reconstruction of the heart of justice itself.

The following recommendations can be made based on these findings and reflections. First, legislators need to establish a specific law on digital identity that is not only oriented towards protecting personal data, but also recognizes digital identity as a distinct legal subject with rights to integrity, autonomy, and protection from algorithmic manipulation. Second, the legal accountability system should be expanded to encompass systemic and algorithmic accountability schemes through a design- and impact-based liability approach, including the possibility of adopting the principle of strict liability for damages caused by autonomous systems. Third, a dedicated institution or digital forensic unit should be established within the criminal justice system that focuses on the detection, verification, and litigation of digital identity crimes committed by or through AI systems. Fourth, the legal education system should reformulate its curriculum to incorporate the study of non-human agency, algorithmic ethics, and post-human criminology as part of its core scientific framework. Fifth, Indonesia needs to develop a roadmap for harmonizing digital identity regulations with international standards such as the GDPR while simultaneously developing institutional capacity capable of responding to the challenges of global, network-based crime. Finally, genuine legal reform must stem from the realization that today's legal world is no longer determined solely by state law, but by a digital ecosystem that has overturned the boundaries between humans and machines, real and virtual, and legitimate and illegitimate.

Ethical Approval

Ethical approval was not required for this study.

Informed Consent Statement

Informed consent was not obtained for this study.

Author Contributions

Tegar Raffi Putra Jumantoro was responsible for conceptualizing the research framework and interpretation of the results. Muhammad Kuttub Firdausy assisted in literature review and supported the final editing process. All authors have reviewed and approved the final version of the manuscript.

Disclosure Statement

The authors declare no conflicts of interest.

Data Availability Statement

The data presented in this study are available upon request from the corresponding author for privacy.

Funding

No external funding was received for the study.

Notes on Contributors

Tegar Raffi Putra Jumantoro

https://orcid.org/0009-0004-9487-8910

Tegar Raffi Putra Jumantoro is an undergraduate law student at the University of Jember, Indonesia, specializing in Private, Economic, and Business Law. With a strong foundation in legal writing, contract drafting, and research, he has authored over ten publications in nationally and internationally recognized journals and presented at multiple international legal conferences. His work primarily focuses on advancing legal education, community empowerment, and sociolegal advocacy, including issues surrounding digital law, anti-corruption frameworks, and human rights protection. Passionate about justice and systemic reform, he is particularly interested in integrating innovative legal strategies to strengthen institutional transparency and rule of law.

Muhammad Kuttub Firdausy

Muhammad Kuttub Firdausy is a law student at the Faculty of Law, University of Jember, Indonesia, with a growing academic and organizational portfolio. Actively involved in legal debates and scientific forums, he has achieved recognition as the first-place winner of a legal debate competition organized by the Forum Kajian Keilmuan Hukum and was a semifinalist in the East Java Legislative Debate Competition. His interests include legal reasoning, public speaking, and team-based advocacy. With experience in moot court competitions and academic organizations, he is committed to developing his competence in legislative studies and legal practice while contributing to youth legal education and community-based empowerment programs.

REFERENCES

Aal, E. B. W. (2022). The Significance of Luhmann's Theory on Organisations for Project Governance. *Project Leadership and Society*, *3*, 1–11. https://doi.org/10.1016/j.plas.2022.100070

Abrar Adhani, Achmad Nashrudin P., & Ade Putranto Prasetyo Wijiharto Tunggali. (2017). *Komunikasi Berkemajuan dalam Dinamika Media dan Budaya*. Asosiasi Pendidikan Ilmu Komunikasi Perguruan Tinggu Muhammadiyah bekerjasama dengan Program Studi Ilmu Komunikasi, Universitas Muhammadiyah Ponorogo dan Buku Litera.

Adnasohn Aqilla Respati, A. D. S. (2024). Analisis Hukum Terhadap Pencegahan Kasus Deepfake Serta Perlindungan Hukum Terhadap Korban. *Media Hukum Indonesia (MHI)*, *2*(2), 586–592. https://doi.org/10.5281/ZENODO.12508126

Agustin, S. M. (2019). Digital Body: Horcrux of Extended Self in Post-Human Era. *Jurnal Komunikasi Indonesia*, *7*(3), 204–214. https://doi.org/10.7454/jki.v7i3.10111

Aini, N., & Lubis, F. (2024). Tantangan Pembuktian dalam Kasus Kejahatan Siber. *Judge: Jurnal Hukum*, *5*(2), 55–63.

Al Kautsar, I., & Muhammad, D. W. (2022). Sistem Hukum Modern Lawrance M. Friedman: Budaya Hukum dan Perubahan Sosial Masyarakat dari Industrial ke Digital. *Sapientia et Virtus*, *7*(2), 84–99. https://doi.org/10.37477/sev.v7i2.358

Alghazali, M. S. D., & Siagian, A. W. (2024). Mutual Legal Assistance as an Instrument for the Eradication of Transnational Crime in the Field of Taxation. *AML/CFT Journal The Journal of Anti Money Laundering and Countering the Financing of Terrorism*, *3*(1), 1–20. https://doi.org/10.59593/amlcft.2024.v3i1.66

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

Ansaroudi, Z. E., Carbone, R., Sciarretta, G., & Ranise, S. (2023). *Control is Nothing Without Trust a First Look into Digital Identity Wallet Trends*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-37586-6_7

Beryl Helga Fredella Hibatulloh. (2025). Upaya Penegakan Hukum Terhadap AI (Artificial Intelligence) Sebagai Subjek Hukum Pidana dalam Perspektif Kriminologi. *Tarunalaw: Journal of Law and Syariah*, *3*(1), 87–98. https://doi.org/10.54298/tarunalaw.v3i01.300

Cahyono, S. T., Erni, W., Hidayat, T., & Trisakti, U. (2025). Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cybercrime) dalam Sistem Peradilan Pidana Indonesia. *Dame Journal Hukum*, *1*(1), 1–23.

Campione, R. (2025). The Legal-Digital Metamorphosis of the Individual. *Philosophies*, *10*(1), 2. https://doi.org/10.3390/philosophies10010002

Cecez-Kecmanovic, D. (2025). Ethics in the World of Automated Algorithmic Decision-Making—A Posthumanist Perspective. *Information and Organization*, *35*(3), 1–16. https://doi.org/10.1016/j.infoandorg.2025.100587

Constantin, N., & Sitorus, F. (2024). Autopoiesis: Komunikasi dan Implementasi pada Era Modern dalam Perspektif Niklas Luhmann. *COMSERVA : Jurnal Penelitian dan Pengabdian Masyarakat*, *4*(8), 2609–2618. https://doi.org/10.59141/comserva.v4i8.2742

Cornelia Riehle. (2022). Europol Report Criminal Use of Deepfake Technology. *Eucrim*. https://eucrim.eu/news/europol-report-criminal-use-of-deepfake-technology/

Danrivanto Budhijanto. (2025). *Teori Hukum Digital (Lex Digitalis)*. Logoz Publishing.

Dwi Kurniawan, K., & Indri Hapsari, D. R. (2022). Pertanggungjawaban Pidana Korporasi Menurut Vicarious Liability Theory. *Jurnal Hukum Ius Quia Iustum*, *29*(2), 324–346. https://doi.org/10.20885/iustum.vol29.iss2.art5

Endang Purwaningsih. (2022). *Metode Penelitian Hukum*. Sonpedia Publishing.

Fajar, M., Kambodji, A. B., & Musdar, I. A. (2023). Implementasi Algoritma Advanced Encryption Standard untuk Pengamanan Data Pengguna Aplikasi Media Sosial VirCle. *Jurnal Algoritma*, *20*(2), 398–409. https://doi.org/10.33364/algoritma/v.20-2.1466

Fauzi, E., & Radika Shandy, N. A. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Jurnal Lex Renaissance*, *7*(3), 445–461. https://doi.org/10.20885/jlr.vol7.iss3.art1

Firman, F. A. (2018). *Kebijakan Pertahanan Cyber Estonia Dalam Merespon Tindakan Cyber Sabotage Oleh Rusia Kepada Estonia*. Universitas Komputer Indonesia.

Gemilang, H. F. (2025). Meninjau Ilmu Digital Forensik Terhadap Bukti Elektronik dalam Tindak Pidana Informasi dan Transaksi Elektronik. *Perahu (Penerangan Hukum): Jurnal Ilmu Hukum*, *12*(2), 45–56. https://doi.org/10.51826/perahu.v12i2.984

Gilani, S. (2021). Bionic Bodies, Posthuman Violence and the Disembodied Criminal Subject. *Law and Critique*, *32*(2), 171–193. https://doi.org/10.1007/s10978-020-09284-6

Ida Bagus Wisnuputra Raditya & I Dewa Gede Dana Sugama. (2024). Analisis Yuridis Asas Fiksi Hukum dari Prespektif Hukum Pidana Dalam Kasus Illegal Logging di Probolingo. *Jurnal Hukum, Politik dan Ilmu Sosial*, *3*(1), 350–359. https://doi.org/10.55606/jhpis.v3i1.3409

Jaya, F., & Goh, W. (2021). Analisis Yuridis Terhadap Kedudukan Kecerdasan Buatan atau Artificial Intelligence Sebagai Subjek Hukum pada Hukum Positif Indonesia. *Supremasi Hukum*, *17*(02), 01–11. https://doi.org/10.33592/jsh.v17i2.1287

Kadek Ayu Widya Arisanthi. (2025). Hak Atas Privasi dalam Pengelolaan Digital Legacy Pascakematian sebagai Wujud Perlindungan Hak Asasi. *Politika Progresif : Jurnal Hukum, Politik dan Humaniora*, *2*(2), 104–113. https://doi.org/10.62383/progres.v2i2.1672

Kadir, Z. K. (2025). Kejahatan Berbasis Identitas Digital: Menggagas Kebijakan Kriminal untuk Dunia Metaverse. *Jurnal Litigasi AMSIR*, *12*(2), 124–137.

Kevin D. Haggerty & Daniel Trottier. (2015). Surveillance and/of Mature: Monitoring Beyond the Human. *Society & Animals*, *23*(4), 400–420.

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. *Science and Engineering Ethics*, *26*(1), 89–120. https://doi.org/10.1007/s11948-018-00081-0

Li, Y. (2019). The California Consumer Privacy Act of 2018: Toughest U.S. Data Privacy Law with Teeth? *Loyola Consumer Law Review*, *32*(1), 177–192.

Luhur, K. B., Trihartono, A., & Hara, A. E. (2025). Navigating Digital Frontiers: Estonia's e-Residency through the Lens of the Eclectic Paradigm. *Jurnal Global Strategis*, *19*(1), 121–142. https://doi.org/10.20473/jgs.19.1.2025.121-142

Mahameru, D. E., Nurhalizah, A., Wildan, A., Haikal, M., & Rahmadia, M. H. (2023). Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas di Indonesia. *Jurnal Esensi Hukum*, *5*(2), 115–131.

Mark Taylor & Mireille Meissner. (2019). *Agency and the Posthuman Shape of Law*. Springer.

Mawlidy, E. R., Primasatya, R. D., & Lorensa, L. (2024). Kemampuan Artificial Intelligence Terhadap Pendeteksian Fraud: Studi Literatur. *Jurnal Studi Akuntansi dan Keuangan*, *7*(1), 89–104.

Muhammad Singgih Imam Wibowo, Akhmad Munawar, & Hidayatullah. (2024). Kendala Teknis dan Hukum dalam Proses Penyidikan Tindak Pidana Siber di Indonesia. *Rewang Rencang: Jurnal Hukum Lex Generalis*, *5*(7), 1–15.

Nimerodi Gulo & Cornelius Dikae Zolohefona Gulo. (2024). Timbulnya Keyakinan Hakim dalam Hukum Pembuktian Perkara Pidana di Peradilan Indonesia. *UNES Law Review*, *6*(3), 8115–8122. https://doi.org/10.31933/unesrev.v6i3

Nitaria Angkasa. (2019). *Metode Penelitian Hukum: Sebagai Suatu Pengantar*. CV Laduny Aliftam.

Osborne, T., & Rose, N. (2024). Against Posthumanism: Notes towards an Ethopolitics of Personhood. *Theory, Culture & Society*, *41*(1), 3–21. https://doi.org/10.1177/02632764231178472

Otoritas Jasa Keuangan. (2025). The Future of Cybersecurity: Threats, Challenges, and Innovations. *Otoritas Jasa Keuangan*. https://institute.ojk.go.id/ojk-institute/id/capacitybuilding/upcoming/4776/the-future-of-cybersecurity-threats-challenges-and-innovations

Patricia Morisa Banfatin, Karolus Kopong Medan, & Debi F.Ng. Fallo. (2024). Pengaturan Hukum Pidana di Indonesia Terhadap Penyalahgunaan Teknologi Artificial Intelligence Deepfake Dalam Melakukan Tindak Pidana Cybercrime. *Pemuliaan Keadilan*, *2*(1), 60–73. https://doi.org/10.62383/pk.v2i1.402

Praja, C. B. E., Nurjaman, D., Fatimah, D. A., & Himawati, N. (2016). Strict Liability Sebagai Instrumen Penegakan Hukum Lingkungan. *Varia Justicia*, *12*(1), 42–62.

Puspita Sari, A., & Harwika, D. M. (2022). Legal Liability of Artificial Intelligence in Perspective of Civil Law in Indonesia. *International Journal of Social Science Research and Review*, *5*(2), 57–60. https://doi.org/10.47814/ijssrr.v5i2.191

Putri, K. V. K. (2021). Kerja Sama Indonesia dengan ASEAN Mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime. *Rewang Rencang: Jurnal Hukum Lex Generalis*, *2*(7), 542–554.

Rahmawati, D. S., Rosadi, S. D., & Cahyadini, A. (2025). Implementasi Pelindungan Data Pribadi Berupa Nomor Induk Kependudukan (NIK) dan Nomor Pokok Wajib Pajak (NPWP) pada Sistem Pemerintahan Berbasis Elektronik Menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Media Hukum Indonesia (MHI)*, *3*(2), 739–749.

Ravizki, E. N. & Lintang Yudhantaka. (2022). Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual dan Tantangan Pengaturan di Indonesia. *Notaire*, *5*(3), 351–376. https://doi.org/10.20473/ntr.v5i3.39063

Ricciardi Celsi, L., & Zomaya, A. Y. (2025). Perspectives on Managing AI Ethics in the Digital Age. *Information*, *16*(4), 318. https://doi.org/10.3390/info16040318

Robertus Robet & U Abdul Rozak R. (2023). Konstruktivisme Bruno Latour dan Implikasinya Terhadap Ide Keagenan Sosiologi. *Masyarakat: Jurnal Sosiologi*, *28*(2), 1–26. https://doi.org/10.7454/mjs.v28i2.13565

Sandoval, M.-P., De Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of Deepfakes to the Criminal Justice System: A Systematic Review. *Crime Science*, *13*(1), 1–16. https://doi.org/10.1186/s40163-024-00239-1

Sarkar, G., & Shukla, S. K. (2023). Behavioral Analysis of Cybercrime: Paving the Way for Effective Policing Strategies. *Journal of Economic Criminology*, *2*, 1–26. https://doi.org/10.1016/j.jeconc.2023.100034

Sih Yuliana Wahyuningtyas, Yerik Afrianto Singgalen, & Enny Widawati. (2025). *Human-Computer Interaction (HCI) dan Portabilitas Data Biometrik dalam Teknologi Imersif*. Atma Jaya Catholic University of Indonesia.

Sirait, Y. H. (2019). General Data Protection Regulation (GDPR) dan Kedaulatan Negara Non-Uni Eropa. *Gorontalo Law Review*, *2*(2), 60–71. https://doi.org/10.32662/golrev.v2i2.704

Tabiu, R., Heryanti, Intan, N., & Safiuddin, S. (2023). Globalisasi dan Kejahatan Transnasional Terorganisasi. *Halu Oleo Law Review*, *7*(1), 99–110. https://doi.org/10.33561/holrev.v7i1.11

Veridas. (2024). Veridas Identity Fraud Report. *Veridas*. https://veridas.com/en/identity-fraud-report/

Wendy, W., Alinurdin, D., & Sekolah Tinggi Teologi SAAT, Malang. (2021). Optimisme yang Tidak Menjanjikan: Kajian terhadap Transhumanisme dari Perspektif Antropologi Kristen. *Veritas: Jurnal Teologi dan Pelayanan*, *20*(1), 21–36. https://doi.org/10.36421/veritas.v20i1.408

Zuchri Abdussamad. (2021). *Metode Penelitian Kualitatif*. Syakir Media Press.

Zul Khaidir Kadir. (2025). Fear and Control: Rethinking Criminal Policy through the Lens of Moral Panic. *International Journal of Law Analytics (IJLA)*, *3*(2), 201–218.