

Reconstructing Cyber Mens Rea Through Electronic Evidence and Algorithmic Accountability

**Antonius Maria Laot Kian, Rizky Pratama Putra Karo Karo,
Selamat Lumban Gaol, Subhan Zein Sgn**

Faculty of Law, Universitas Dirgantara Marsekal Suryadarma, Jakarta, Indonesia
antoniusmarialaotkian2020@gmail.com

Abstract

This study examines how mens rea in Indonesian cybercrime can be established through electronic evidence and algorithmic analysis, focusing on the legal standards governing the transition from digital traces to proof of criminal intent. Using normative legal research with statutory, case, conceptual, and comparative approaches, the study analyses Indonesian criminal evidence law and the ratio decidendi of Tangerang District Court Decision No. 1240/Pid.Sus/2022/PN Tng (Indra Kenz), with reference to comparative developments in other jurisdictions. The findings demonstrate that Indonesian law recognizes the legality and authenticity of electronic evidence but does not yet provide sufficiently specific standards for evaluating the inferential validity and evidentiary weight of technical or algorithmic outputs in establishing mens rea. The Indra Kenz decision shows that intent is reconstructed cumulatively from digital content, electronic communications, account activity, financial transactions, and analytical reports, creating a potential conflation between factual digital evidence, technical inference, and legal judgment. The novelty of this study lies in developing a three-layer cyber mens rea framework that integrates criminal-law doctrine with agentic computational law and algorithmic accountability: digital facts must satisfy legality, authenticity, integrity, and relevance; technical or algorithmic inferences must be transparent, explainable, auditable, and contestable; and the final determination of mens rea must remain with the judge based on the totality of admissible evidence. The framework provides a normative basis for regulating algorithmic evidence while safeguarding the presumption of innocence, due process, and meaningful human control over criminal responsibility.

Keywords: Algorithmic Accountability; Cyber Mens Rea; Electronic Evidence; Presumption of Innocence

1. INTRODUCTION

Advances in information technology have transformed the nature of criminal offenses from those originally based in the physical realm to those based in the digital realm.¹ Cybercrime not only introduces new methods of operation but also poses new challenges to the criminal evidentiary system.² One of the most complex issues is proving the element of criminal intent (*mens rea*) in cybercrimes.³ In conventional criminal offenses, the perpetrator's intent can generally be reconstructed through physical actions,⁴ witness testimony, or the circumstances surrounding the criminal act. This differs from cybercrimes, which are committed through electronic systems, computer networks, and software, meaning that the perpetrator's behavioral

¹ Claudia Agatha and R. Rahaditya, "Fragmented Digital Forensic Standards in Indonesian Criminal Evidence," *Indonesian Journal of Law and Economics Review* 21, no. 2 (May 20, 2026): 1–11, <https://doi.org/10.21070/ijler.v21i2.1558>.

² Yevi Mulyana Erawan, Novayandra Arinuridin, and Muhammad Dwi Yuliandy, "Tantangan Pembuktian Kejahatan Siber (Cybercrime) Dalam Peradilan Pidana," *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 4, no. 2 (2026): 3069–75, <https://doi.org/10.61104/alz.v4i2.4828>.

³ Muhammad Candra and Muhammad Ruhly Kesuma Dinata, "Penegakan Hukum Terhadap Tindak Pidana Penyebaran Berita Hoaks Melalui Media Sosial," *Arus Jurnal Sosial Dan Humaniora* 5, no. 2 (August 1, 2025): 1577–86, <https://doi.org/10.57250/ajsh.v5i2.1373>.

⁴ Aris Munandar Ar et al., "Peran Niat (*Mens rea*) Dalam Pertanggungjawaban Pidana Di Indonesia," *Jimmi: Jurnal Ilmiah Mahasiswa Multidisiplin* 1, no. 3 (October 27, 2024): 240–52, <https://doi.org/10.71153/jimmi.v1i3.140>.

traces are primarily recorded in the form of digital data, metadata, system logs, and other electronic artifacts.

This difficulty is further compounded by the fact that electronic evidence has characteristics that differ from those of conventional evidence. The existence of electronic evidence is highly dependent on the processes of extraction, authentication, and interpretation using specific forensic software. As a result, the link between digital evidence and the perpetrator's mental state cannot always be proven directly. This issue is important because modern criminal law continues to require the presence of fault as the basis for criminal liability through the principle of *actus non facit reum nisi mens sit rea*. A person cannot be held criminally liable merely because harmful consequences have occurred; rather, it must be proven that the act was committed with a certain level of awareness and intent.⁵

Indonesian positive law has accommodated these developments through various legislative instruments, including Law No. 1 of 2024 on the Second Amendment to the Law on Electronic Information and Transactions, Law No. 1 of 2023 on the Criminal Code, the new Code of Criminal Procedure, and Law No. 27 of 2022 on Personal Data Protection. These various regulations provide a normative basis for the enforcement of cyber law, but they do not yet address in detail how the subjective element of intent must be proven when an act is committed through an electronic system in which part of the process occurs automatically.

This study raises several questions. What standard must the prosecutor meet to prove the phrase "intentionally" with respect to acts committed through an electronic system? How can a judge conclude the perpetrator's mental state from a series of digital traces, some of which are probabilistic in nature and generated through forensic software analysis? Can electronic evidence obtained through extraction using a specific algorithm or the results of transaction pattern analysis conducted by an institution such as PPATK be treated as direct grounds for concluding that there was intent? This issue has become increasingly relevant since the 2025 Criminal Procedure Code recognized electronic evidence as a valid form of evidence and adopted the exclusionary rule for evidence that is inauthentic or obtained unlawfully. Nevertheless, Indonesian criminal procedure law still does not provide clear parameters regarding how the probative value of electronic evidence should be applied to prove subjective elements such as *mens rea*.

The urgency of this issue is evident in the practice of cybercrime adjudication in Indonesia. One relevant case is the Tangerang District Court's Decision No. 1240/Pid.Sus/2022/PN Tng regarding the defendant Indra Kesuma (Indra Kenz). In that case, the defendant was found guilty of the criminal offense of disseminating misleading information that harmed consumers in electronic transactions, as well as the criminal offense of money laundering through promotional activities for the Binomo binary options platform. The verdict subsequently became final after all legal appeals were rejected. This case demonstrates that the construction of the element of intent plays a central role in proving crimes involving electronic systems.

⁵ Sir William Blackstone, *Commentaries on the Laws of England* (Oxford: Clarendon Press, 1976); Jerome Hall, *General Principles of Criminal Law* (Indianapolis: Bobbs-Merrill, 1960).

The significance of this case becomes even more apparent when compared to the ruling of the Bale Bandung District Court, No. 576/Pid.Sus/2022/PN Blb, in the case of Doni Muhammad Taufik (Doni Salmanan). Although the two cases share relatively similar characteristics and *modus operandi*, there are differences in the legal reasoning and the application of criminal liability. This phenomenon indicates that proving the subjective elements in cybercrime cases still leaves considerable room for interpretation. This situation has the potential to lead to inconsistencies in the application of the law and uncertainty regarding the parameters for proving *mens rea* in cases based on electronic evidence.

Studies on cyber law and the evidence of digital crimes have grown rapidly in recent years, but they are still fragmented into three main areas. The first area focuses on cyber attribution. For example, Pavliukh and Sanzharova (2024) explain the relationship between technical attribution, public attribution, and legal attribution in determining the identity of perpetrators and legal responsibility for cyber attacks.⁶ The study makes an important contribution to the issue of who is responsible for a digital attack, but it doesn't explain how the subjective element of *mens rea* should be proven once the perpetrator's identity has been found.

The second cluster focuses on the regulation of electronic evidence and cyber law enforcement. Aljundani and Sinaga (2025) point out that the evidentiary regime in the Electronic Information and Transactions Law has provided a sufficient normative basis for law enforcement against illegal access, but it still faces technical and institutional obstacles.⁷ The study shows that the enforcement of illegal access laws already has a relatively adequate normative basis, but it still faces various technical and institutional obstacles. However, the study hasn't addressed how the element of intent is proven through electronic evidence and how judges construct the perpetrator's *mens rea*.

Similarly, Karo and Prasetyo (2025) highlight the legal responsibility of electronic system providers in the financial technology ecosystem.⁸ The study highlights the relationship between the operation of electronic systems, personal data protection, regulatory compliance, and the legal accountability of digital service providers. However, the study has not examined how the *mens rea* element is proven in cybercrime cases or how judges draw conclusions about intent from electronic evidence presented in court. That said, while enriching the discourse on the legality of electronic evidence and compliance of digital systems, both studies have yet to explain how judges link electronic evidence to proving intent as a requirement for criminal liability.

Meanwhile, international literature developments are starting to focus on issues like algorithmic governance and AI-assisted criminal adjudication, which means using artificial intelligence, forensic software, and analytics systems to support investigations and criminal

⁶ O.A. Pavliukh and H.F. Sanzharova, "Crime Attribution as a Critical Cybersecurity Issue," *Juridical Scientific and Electronic Journal*, no. 9 (2024): 303–6, <https://doi.org/10.32782/2524-0374/2024-9/72>.

⁷ Arifuddin Aljundani and Niru Anita Sinaga, "Penegakan Hukum Terhadap Pelaku Tindak Pidana Siber Tentang Akses Ilegal Di Indonesia," *Lex Laguens: Jurnal Kajian Hukum Dan Keadilan* 3, no. 2 (2025): 176–93, <https://doi.org/10.08221/lexlaguens.v3i2.271>.

⁸ Rizky Karo Karo and Teguh Prasetyo, "The Provision of Licensed Financial Technology Lending From The Perspective of Cyber Law and Criminal Law in Indonesia," *Pena Justisia: Media Komunikasi Dan Kajian Hukum* 24, no. 1 (September 30, 2025): 7263–80, <https://doi.org/10.31941/pj.v24i2.6559>.

court decision-making. Various studies show that using algorithms can boost the efficiency of spotting crime patterns and analyzing digital evidence, but it also raises concerns about transparency, explainability, algorithmic bias, and protecting due process. The main focus of those studies still revolves around the accountability of artificial intelligence systems and algorithmic governance, rather than on reconstructing the *mens rea* doctrine as a subjective element of criminal liability. In other words, international literature has talked a lot about how algorithms generate or process evidence, but it hasn't answered a more fundamental question: how the results of algorithmic analysis can be translated into proof of intent without shifting the presumption of innocence.

So, there's a clear theoretical gap in the literature. Research on cyber attribution explains how perpetrators are identified, studies on digital evidence look at the legality and strength of proof of digital data, while research on algorithmic governance focuses more on the transparency and accountability of AI systems. These three areas haven't been integrated into a framework that explains how the classic *mens rea* doctrine is reconstructed when proving fault relies on inferences drawn from digital evidence and algorithmic processes. As a result, there aren't yet conceptual parameters judges can use to distinguish between probabilistic technical inferences and proof of intent that meets criminal law standards.

Based on this gap, this study offers novelty in two aspects. First, it integrates the *mens rea* theory in criminal law with the perspective of agentic computational law and algorithmic accountability to build a conceptual framework for cyber *mens rea*. Second, it tests this framework through an analysis of the *ratio decidendi* of the Tangerang District Court Decision Number 1240/Pid.Sus/2022/PN Tng (Indra Kenz), so it not only explains how electronic evidence is used in court practice, but also formulates normative standards to ensure that the use of algorithmic inference stays in line with the presumption of innocence and the principle of due process of law.

2. METHOD

This writing is normative legal research, which treats law as a system of norms studied internally rather than as a social phenomenon measured empirically.⁹ The choice follows from the character of the issues examined, which are normative and doctrinal: the regulation of proving the *mens rea* element of cyber offences, and the *ratio decidendi* of a final judgment construing that element. Such issues are not answered by survey or experiment; they demand careful analysis of positive norms, legal doctrine, legal principles, and jurisprudence.

Four approaches are combined. The statutory approach is used to examine the legislation governing cyber offences and their proof, including the 1945 Constitution, the Electronic Information and Transactions Law and its amendments, the National Criminal Code, the new Criminal Procedure Code, the Personal Data Protection Law, and the Anti-Money-Laundering Law. The case approach is used to read final decisions in order to find their *ratio decidendi*, centred on the Tangerang District Court judgment in the Indra Kenz case, in conjunction with

⁹ Sidi Ahyar Wiraguna, "Metode Normatif Dan Empiris Dalam Penelitian Hukum: Studi Eksploratif Di Indonesia," *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum* 3, no. 3 (November 30, 2024): 57–65, <https://doi.org/10.59818/jps.v3i3.1390>.

the Banten High Court and Supreme Court decisions affirming it, and compared with the Bale Bandung judgment in the Doni Salmanan case. The conceptual approach dissects the concepts of *mens rea*, *actus reus*, proof, criminal liability, agentic computational law, and algorithmic accountability, drawing on doctrine in both the common-law and civil-law traditions. The comparative approach considers how other jurisdictions, in particular the United States, the European Union, the United Kingdom, Germany, and Singapore, address similar challenges, so that relevant lessons may be drawn for Indonesian reform rather than transplanted wholesale. Thus, these four approaches form a single analytical framework: statutory provisions are used to establish the normative framework; court decisions are used to examine their application; conceptual approaches are used to test the theoretical basis and construct legal arguments; and comparative law is used to enrich and test alternative solutions to the issues identified.

The selection of the Indra Kenz and Doni Salmanan cases was based on criteria relevant to the focus of this study, namely the common characteristics of electronic transaction-based criminal offenses, the use of digital media in the commission of the acts, the involvement of binary options platforms, and the issues of criminal liability and money laundering offenses that must be assessed through a body of electronic evidence. Both cases also hold analytical value because they stem from court rulings that have gone through the judicial process and demonstrate differences in the legal reasoning applied to cases with relatively similar characteristics. The Indra Kenz case is highlighted as the primary case because its ruling provides an opportunity to analyze how electronic evidence is used to establish the element of intent, while the Doni Salmanan case serves as a comparative case to test the consistency of that legal reasoning. The comparison of the two cases is not intended to suggest that they are identical, but rather to identify similarities and differences in the legal facts, evidence, judicial reasoning, and the construction of subjective elements. Using these criteria, the analysis of the two cases is not merely illustrative but serves as a targeted case comparison to examine the presence or absence of patterns, consistency, and differences in legal reasoning regarding the proof of *mens rea* in cybercrimes.

The legal materials consist of two layers. Primary materials comprise the legislation and judicial decisions named above, together with relevant international instruments such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European General Data Protection Regulation, and the European Union Artificial Intelligence Act. Secondary materials comprise academic books, scholarly journal articles, and reports of credible institutions that address the intersection of criminal evidence, artificial intelligence, and the basic rights of suspects. All of these materials are analysed qualitatively through deductive reasoning, moving from general normative premises to specific conclusions about the problem, and interpreted grammatically, systematically, historically, and teleologically so that the meaning of the norms is not only internally consistent but also responsive to the realities posed by digital technology.

The research analysis framework is done in three stages. In the first stage, a normative analysis is carried out on the provisions of laws and regulations to identify the legal standards regarding proving the element of intent in cybercrime. In the second stage, an analysis is conducted on the *ratio decidendi* of court decisions to see how judges draw inferences about *mens rea* from

electronic evidence, including the use of digital traces, financial transaction analysis reports, and digital forensic examination results. In the third stage, the results of this analysis are evaluated using two conceptual frameworks, namely agentic computational law and algorithmic accountability. The agentic computational law perspective is used to assess whether the evidence process still keeps humans as the main subjects of criminal responsibility when actions are carried out through automatic or semi-automatic digital systems. Meanwhile, the algorithmic accountability perspective is used to evaluate whether the use of forensic software, algorithm-based analysis, and electronic evidence meets the principles of transparency, explainability, auditability, and the defendant's right to challenge the analysis results. Through these two frameworks, the study examines whether the evidence construction applied by the courts still aligns with the presumption of innocence and the principle of due process of law, while also serving as a basis for formulating a conceptual reconstruction of cyber *mens rea*.

All legal materials are analyzed qualitatively through deductive reasoning using grammatical, systematic, historical, and teleological interpretation methods to produce a doctrinal reconstruction regarding the proof of *mens rea* in cybercrimes that is responsive to the development of digital technology without disregarding fundamental principles of criminal law.

3. RESULTS AND DISCUSSION

3.1 The Ontological Crisis of *Mens rea* in the Digital Sphere

The classical formulation of the guilty mind rests on three assumptions that were accepted for centuries without much argument. The first is consciousness: the offender is a conscious being who knows what they are doing and can anticipate the consequences.¹⁰ The second is free will: the choice to do wrong is made autonomously, not through mechanical coercion or external determination.¹¹ The third is individuality: there is a single subject who can be identified as the owner of the wrongful intent and held to account before a court.¹² These assumptions remain robust so long as crime keeps a familiar human shape: the robber who plans, the fraudster who schemes, the killer who nurses a grievance. Cyberspace cracks them one by one.

The shift of human activities into digital spaces changes that assumption. In cybercrime, the actions of perpetrators are often mediated by software, computer networks, automated systems, or even artificial intelligence. As a result, the relationship between the perpetrator, their actions, and the consequences no longer happens in a straight line like in conventional crimes. Consider the simplest example: a distributed denial-of-service attack launched through a botnet. An offender in one country spreads malware that quietly infects hundreds of thousands of devices whose owners have no idea their computers have been conscripted. When the attack executes, no conscious command is issued in real time; everything runs automatically on instructions

¹⁰ Nelson Cowan et al., "Theories of Consciousness from the Perspective of an Embedded Processes View.," *Psychological Review* 132, no. 1 (January 2025): 76–106, <https://doi.org/10.1037/rev0000510>.

¹¹ Ragıp Baris Erman, "Perspective Chapter: Criminal Responsibility," in *Criminal Behavior - The Underlyings, and Contemporary Applications* (IntechOpen, 2023), <https://doi.org/10.5772/intechopen.1002345>.

¹² Rina Zejneli and Besa Arifi, "Criminal Responsibility (Insanity Defense)," *SEEU Review* 17, no. 2 (December 1, 2022): 120–38, <https://doi.org/10.2478/seeur-2022-0092>.

implanted long before.¹³ Where does the *mens rea* lie, at the moment the malware was written, at deployment, or at execution without the offender's active presence? The problem doubles when artificial intelligence enters as an actor, in the phenomenon now called AI-generated crime, where non-human systems make operational decisions independently, selecting targets, choosing methods, and adapting to a victim's response.¹⁴ Such a system does not "intend" in any morally recognised sense, yet its consequences can be very real.

What complicates matters further is the long and layered causal chain typical of cyber offences.¹⁵ In conventional crime, the link between intent, act, and result is relatively easy to trace.¹⁶ In cyberspace, an attack may involve exploit developers, access vendors, botnet operators, and brokers, each holding only a small fragment of the whole,¹⁷ so that the existing doctrine of participation (*deelneming*) was never designed for this extreme fragmentation of roles. The crisis, then, is not only the technical question of how to prove intent digitally; it is the ontological loss of the conscious, free, and identifiable human subject that has long been the centre of gravity of criminal law.

This situation not only raises ontological questions about the existence of a legal subject, but also brings practical consequences for proof in criminal proceedings. When the connection between the perpetrator and the outcome can no longer be observed directly, proving *mens rea* shifts from behavior-based evidence to inference-based evidence from digital traces. Judges no longer mainly evaluate confessions, physical actions, or direct testimony, but have to draw conclusions about intent from metadata, system logs, electronic communications, digital transaction histories, or forensic software analysis results. Thus, the higher the level of automation in a system, the greater the reliance of the evidentiary process on technical interpretation of electronic evidence.

Hildebrandt frames this loss with unusual precision. Her thesis is that law, as a social institution,¹⁸ must be rethought ontologically when it confronts computational systems, because classical concepts such as *mens rea*, agency, and legal subjectivity cannot simply be

¹³ Slamet Slamet, "Pendeteksi Botnet Malware DDOS Untuk Mencegah Serangan Distributed Denial of Service," *SPIRIT: Journal Of Computing and Cybernetic System* 16, no. 2 (November 30, 2024), <https://doi.org/10.53567/spirit.v16i2.361>; Abeer Abd Alhameed Mahmood and Wasan Hashim Al Masoody, "A Comprehensive Analysis of Botnet Detection and Distributed Denial of Service Attacks: The Function of Deep Learning and Machine Learning Methods," *American Journal of Technology Advancement* 2, no. 2 (2025): 6–23, <https://doi.org/10.31150/ajta.v2i2.1089>; Metehan Gelgi et al., "Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques," *Sensors* 24, no. 11 (June 1, 2024): 3571, <https://doi.org/10.3390/s24113571>.

¹⁴ Ildar Begishev et al., "Research of Artificial Intelligence as a Subject of Crime," ed. I. Abdullayev et al., *E3S Web of Conferences* 449 (November 16, 2023): 03004, <https://doi.org/10.1051/e3sconf/202344903004>; Wawan Fransisco, "Drafting Laws for The Lifeless: A Legal Framework for Criminal Liability and Punishment for Artificial Intelligence," *Jurnal Hukum Dan Peradilan* 14, no. 3 (November 30, 2025): 701–18, <https://doi.org/10.25216/jhp.14.3.2025.701-718>.

¹⁵ Fitri Novia Heriani, "Menakar Pertanggungjawaban Hukum Penggunaan Artificial Intelligence," *Hukumonline*, 2026, <https://www.hukumonline.com/berita/a/menakar-pertanggungjawaban-hukum-penggunaan-artificial-intelligence-lt69dcd592de37e/>.

¹⁶ Abdul Aziz, "Rekonstruksi Hukum Penyalahgunaan Artificial Intelligence (AI) Dalam Konten Kesusilaan Dan Pencemaran Nama Baik," *Jurnal Hukum Lex Generalis* 6, no. 7 (2026): 1–30, <https://doi.org/10.56370/jhlg.v6i7.3209>.

¹⁷ Constantinos Patsakis, David Arroyo, and Fran Casino, "The Malware as a Service Ecosystem," 2025, 371–94, https://doi.org/10.1007/978-3-031-66245-4_16.

¹⁸ Galih Orlando, "Hukum Sebagai Kontrol Sosial Dan Social Engineering," *Tarbiyah Bil Qalam : Jurnal Pendidikan Agama Dan Sains* 7, no. 1 (July 15, 2023), <https://doi.org/10.58822/tbq.v7i1.111>; Wegestin Lagus, Salma Salma, and Bakhtiar Bakhtiar, "The Dynamics of Social Institutions in Family Law: Understanding Values, Norms, and Their Functions," *Al-Qanun: Jurnal Kajian Sosial Dan Hukum Islam* 6, no. 2 (October 2, 2025): 120, <https://doi.org/10.58836/al-qanun.v6i2.24685>.

applied by analogy to the algorithmic domain. Computational technology changes the very way humans intend, act, and become legal subjects, and a law that fails to reconceptualise itself risks being replaced by what she calls code-driven law, in which conduct is governed entirely by code without the intervention of conventional law.¹⁹ Her project, carried out under the European Research Council programme on counting as a human being in the era of computational law, asks the ontological question directly: how does the human remain a legal subject, and not merely a data point, once decisions are mediated by machines?²⁰ That question is the doctrinal pressure point of this article, because the proof of intent in a cyber case is exactly the moment at which a defendant is, or is not, treated as a full subject capable of contesting the construction placed upon their digital traces.

This situation not only raises ontological questions about the existence of a legal subject, but also brings practical consequences for proof in criminal proceedings. When the connection between the perpetrator and the outcome can no longer be observed directly, proving *mens rea* shifts from behavior-based evidence to inference-based evidence from digital traces. Judges no longer mainly evaluate confessions, physical actions, or direct testimony, but have to draw conclusions about intent from metadata, system logs, electronic communications, digital transaction histories, or forensic software analysis results. Thus, the higher the level of automation in a system, the greater the reliance of the evidentiary process on technical interpretation of electronic evidence.

These changes directly affect the standard of legal proof. In conventional cases, the connection between an act and the state of mind can be built through a series of facts that are relatively easy to verify, but in cyber cases, that connection is often derived through inferences produced by algorithmic analysis. As a result, there's a risk that a defendant's intent is no longer proven independently, but inferred from probabilities generated by forensic software or analytical systems, including analysis of financial transaction patterns or correlations in digital activities. This shift could weaken the presumption of innocence if technical analysis results are treated as a direct representation of *mens rea* without giving the defendant a fair chance to test the validity of the methods, assumptions, or accuracy of the algorithms used.

This issue aligns with Hildebrandt's thinking, who states that the development of computational law demands a reconstruction of fundamental criminal law concepts, including agency, legal subjectivity, and *mens rea*. According to Hildebrandt, using computational systems has the potential to shift law toward code-driven regulation, which is a situation where decision-making is increasingly determined by code and algorithm logic rather than legal reasoning itself. In the context of criminal evidence, this risk arises when judges accept algorithmic analysis results as a basis for attributing intent without critically examining how they were formed. Therefore, the main issue isn't just whether algorithms can help uncover the facts, but how to ensure that using algorithms still keeps humans as the main subject of criminal

¹⁹ Marina Teller, "The Contribution of Law in the Regulation of Artificial Intelligence: Thinking about Algorithmic Democracy," *Journal of Artificial Intelligence for Sustainable Development* 1, no. 1 (January 1, 2024): 1–5, <https://doi.org/10.69828/4d4kmc>.

²⁰ Commission European, "Counting as a Human Being in the Era of Computational Law (CoHuBiCoL)," CORDIS – Community Research and Development Information Service, January 1, 2019, <https://doi.org/10.3030/788734>.

responsibility and ensures that proving *mens rea* still meets the principles of due process of law and the presumption of innocence.

Thus, the ontological crisis of *mens rea* in the digital realm doesn't just stop at changes in the character of the offender or the technology used, but directly alters how courts construct intent. This relationship forms the basis of the analysis in the next section, which looks at how Indonesian courts attribute *mens rea* through electronic evidence and how far these practices remain consistent with the fundamental principles of criminal law.

3.2 The Indonesian Regime for Proving Cyber *Mens rea*

In Indonesian doctrine, the guilty mind takes two principal forms, intent (*dolus*) and negligence (*culpa*).²¹ Intent, following the classical *Memorie van Toelichting*, is rendered as *willens en wetens*,²² willing and knowing, and is subdivided into intent as purpose (*dolus directus*), intent with certainty, and intent with awareness of possibility (*dolus eventualis*).²³ The principle that there is no punishment without fault, *geen straf zonder schuld*,²⁴ is now made explicit in Article 36 paragraph (1) of the National Criminal Code, which states that no person who commits an offence is punished without fault.²⁵ Most cyber offences require intent: the fixed phrase “with intent and without right” runs through Articles 27 to 35 of the Electronic Information and Transactions Law and Articles 322 to 325 of the National Criminal Code, the latter criminalising illegal access to a computer or electronic system.

In the context of cybercrime, this principle is reflected in the formulation of the elements 'intentionally and without rights,' which is a characteristic of most offenses under the Information and Electronic Transactions Law as well as the provisions on illegal access to electronic systems in the National Penal Code. So, even though the object of the crime has shifted to the digital space, proving the subjective element in the form of *mens rea* is still a key requirement before someone can be held criminally responsible.

The procedural frame is the negative statutory system of proof (*negatief wettelijke bewijstheorie*), historically in Article 183 of the 1981 Code and now in Article 252 of KUHAP 2025, under which a judge may not impose punishment unless, with at least two lawful items of evidence, the judge is convinced that an offence occurred and that the defendant is guilty.²⁶ The system sets two cumulative conditions, an objective minimum of two lawful items of

²¹ Dian Rusmana, Numan Sofari Hafid, and Syahrul Anwar, “Analisis Delik *Culpa* Dan Pertanggungjawaban Pidana Atas Kelalaian Pejabat Negara Dalam Perkara Korupsi Melalui Studi Putusan 68/Pid.Sus-TPK/2025/PN Jkt Pst.,” *Mahkamah : Jurnal Riset Ilmu Hukum* 2, no. 4 (December 19, 2025): 127–51, <https://doi.org/10.62383/mahkamah.v2i4.1333>.

²² Jun Triono Pakpahan, Elly Sudarti, and Erwin Erwin, “Pertanggungjawaban Pidana Perbuatan Ujaran Kebencian Yang Berkonten SARA Dalam Perspektif Peraturan Perundang-Undangan,” *Journal of Law, Education and Business* 2, no. 2 (September 30, 2024): 851–71, <https://doi.org/10.57235/jleb.v2i2.2540>.

²³ Vaulus Julianta Nano, Tahasak Sahay, and Claudia Yuni Pramita, “Analisis Teoritis *Dolus* Dan *Culpa* Dalam Konsep Kesalahan Sebagai Dasar Pertanggungjawaban Pidana,” *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 4, no. 2 (2026): 6241–51, <https://doi.org/10.61104/alz.v4i2.5100>.

²⁴ I Made Walesa Putra, “Asas Kesalahan Terkait Pertanggungjawaban Pidana Atas Tindak Pidana Dalam Pelaksanaan Jabatan Notaris,” *Acta Diurnal Jurnal Ilmu Hukum Kenotariatan* 8, no. 1 (2024): 116–31, <https://doi.org/10.23920/acta.v8i1.1958>.

²⁵ Kharisma Wulan Fadhila, “Reformasi Hukum Pidana Dan Pertanggungjawaban Korporasi Dalam UU KUHP 2023,” *Action Research Literate* 8, no. 3 (March 25, 2024): 649–57, <https://doi.org/10.46799/ar.v8i3.277>.

²⁶ Ahmad Bagus Aditia and Muchamad Iksan, “The Relevance of Judicial Beliefs in the Negative Proof System of Article 183 of the Criminal Procedure Code: Analysis of Surabaya District Court Decision Number 454/Pid.B/2024/Pn.Sby,” *Academia Open* 10, no. 2 (December 12, 2025), <https://doi.org/10.21070/acopen.10.2025.12995>.

evidence and a subjective conviction built upon them.²⁷ KUHAP 2025 widens the catalogue: Article 235 paragraph (1) now lists eight categories of evidence, witness testimony, expert testimony, documents, the defendant's statement, physical evidence, electronic evidence, the judge's observation, and anything usable for proof in court so long as it is not unlawfully obtained, while Article 242 defines electronic evidence broadly to include electronic information, electronic documents, and electronic systems connected with an offence.²⁸ Crucially, Article 235 paragraph (5) codifies the exclusionary rule: evidence declared inauthentic or unlawfully obtained may not be used and carries no probative force.

Electronic evidence is the principal gateway through which this regime meets the cyber offence, and its ontology is distinctive. Digital material is easily altered, easily duplicated, and its authenticity depends on metadata that systems generate automatically;²⁹ the Electronic Information and Transactions Law therefore makes electronic information and documents and their printouts lawful evidence under Article 5 paragraph (1) and imposes the material requirements of authenticity, integrity, and availability under Article 6.³⁰ For the subjective element, doctrine proceeds along two routes. The direct route looks for material that openly displays the offender's state of mind, for instance, a chat message in which intent is expressed in so many words. The indirect or circumstantial route infers the inner attitude from a chain of digital facts, a suspicious pattern of financial transactions, an access history, or file metadata showing the time and place of creation. The second route dominates the practice of cyber adjudication, and it is also the route most exposed to the accountability problem that Pasquale identifies, because the inference rests on outputs that the defendant can rarely inspect.

The interaction between these two legal frameworks demonstrates both continuity and normative boundaries. The ITE Law establishes the basis for the existence and nature of electronic evidence, while the Criminal Procedure Code provides the framework for its use in criminal evidentiary proceedings. The relationship between the two has not yet extended to regulations concerning the process of inferring from digital facts to conclusions regarding *mens rea*. Positive law has regulated admissibility and certain aspects of reliability, but has not yet provided specific standards regarding inferential validity that is, whether the method of reasoning that links digital facts to the defendant's mental state is legally justifiable.

The issue becomes more complex when the National Criminal Code is considered in relation to these two instruments. The National Criminal Code affirms that *culpability* is the basis for criminal punishment; thus, the proof of a criminal offense must still include the subjective element if it is specified in the relevant offense.⁶ The Criminal Code thus determines what must be proven, while the Criminal Procedure Code determines how that proof is to be established. The ITE Law provides a legal framework regarding the nature of electronic

²⁷ Ariel Alexander et al., "Analisis Yuridis Kekuatan Pembuktian Dalam Putusan Pengadilan Negeri Praya," *Syntax Literate; Jurnal Ilmiah Indonesia* 10, no. 10 (October 4, 2025): 8262–75, <https://doi.org/10.36418/syntax-literate.v10i10.61788>.

²⁸ Muhammad Raihan Nugraha, "Jenis Alat Bukti Sah Menurut KUHAP Baru," *Hukumonline*, 2026, <https://www.hukumonline.com/klinik/a/jenis-alat-bukti-sah-menurut-kuhap-baru-lt657ae25924ac9/>.

²⁹ A. A. Dmitrieva and P. S. Pastukhov, "Concept of Electronic Evidence in Criminal Legal Procedure," *Journal of Digital Technologies and Law* 1, no. 1 (March 16, 2023): 270–95, <https://doi.org/10.21202/jdtl.2023.11>.

³⁰ Nursanti Mardiyati, "Keabsahan Hukum Fitur Pengaduan Shopee Sebagai Bukti Elektronik Dalam E-Commerce," *Jurnal USM Law Review* 9, no. 1 (January 27, 2026): 50–74, <https://doi.org/10.26623/julr.v9i1.12896>.

evidence used to prove acts in the digital realm. These three instruments actually form a single normative framework. However, this framework is not yet fully integrated at the methodological level of proving *mens rea*.

This fragmentation becomes even more apparent when electronic evidence originates from technical processing. System logs, metadata, communication histories, transaction patterns, and device extraction results are digital facts that can be used as evidence. The results of link analysis, pattern recognition, or financial transaction analysis fall into a different category because they are the result of processing these facts. The distinction between digital facts and the results of technical inference has not yet been clearly defined in Indonesian criminal procedure law. Consequently, there is a possibility that the results of technical processing may be treated as if they had the same status as the underlying digital facts.

At this point, the Personal Data Protection Act adds another dimension to Indonesia's legal framework. Personal data protection is not only about whether data can be used, but also about how data is processed and how the interests of data subjects are protected. Provisions regarding the processing of personal data set limits on the use of data, including when processing is carried out in certain ways that may affect the data subject.⁷ The issue is that the Personal Data Protection Act was not designed as a law governing criminal evidence. Its relationship with the Criminal Procedure Code and the Electronic Information and Transactions Act is therefore complementary, not substitutive. The Personal Data Protection Act establishes principles for the protection of data processing, while the Criminal Procedure Code determines the value and use of evidence in criminal proceedings.

This interaction raises normative issues that have not yet been fully resolved. Personal data may be lawfully obtained and processed using technically sound methods, but the results of such processing do not necessarily automatically serve as proof of *mens rea*. Conversely, violations of procedures for obtaining or processing data may affect the legitimacy of its use in criminal proceedings. Thus, the issue of proving *mens rea* through electronic evidence lies at the intersection of the legality of evidence collection, the reliability of evidence, data protection, and the sufficiency of inferences regarding the element of fault.

This situation demonstrates that Indonesia's positive law has not yet established a comprehensive standard. The Criminal Code (KUHP) provides a substantive framework regarding criminal liability. The Criminal Procedure Code (KUHAP) establishes the structure of proof and the requirements for the use of evidence. The ITE Law recognizes electronic evidence and sets forth requirements for its admissibility. The PDP Law sets limits on the processing of personal data. Each instrument serves a different function and, in general, can complement one another. Fragmentation arises because there are no provisions that explicitly link all four to a more specific question: when can valid and authentic digital evidence be deemed sufficient to establish a judge's conviction regarding the existence of intent?

The absence of such standards has consequences for judicial practice. Judges must ultimately establish a link between electronic evidence and *mens rea* through reasoning based on the totality of the evidence. In cases with strong digital evidence, this process can lead to convincing conclusions. Problems arise when some of these conclusions stem from algorithmic

processing or technical analysis that cannot be fully challenged by the defendant. In such circumstances, there is a risk that the technical validity of an output will be mistakenly taken to simultaneously establish the truth of the legal conclusions drawn from that output.

The distinction between these two must be maintained. The authenticity of evidence merely addresses whether the submitted data genuinely originates from the claimed source and has not undergone alterations that compromise its integrity. The reliability of the method addresses whether the data processing can produce trustworthy findings. Proving *mens rea* addresses a different question, namely whether the totality of the evidence shows that the defendant knew of and intended the act or consequence that constitutes the criminal offense. These three issues cannot be merged into a single conclusion.

A comparison with several other jurisdictions shows that this issue has been addressed through different testing mechanisms. The United States, for example, has developed a test for the reliability of scientific methods through the Daubert standard. The European Union has made transparency and accountability key components of its regulations on automated processing through the GDPR and on artificial intelligence systems through the Artificial Intelligence Act. These developments cannot be directly applied to the Indonesian legal system. The key takeaway lies in the need to distinguish between the admissibility of data, the reliability of the methods yielding an analysis, and the legal weight of the conclusions drawn from that analysis.

Based on this analysis, the legal issue in Indonesia does not lie in the absence of a legal basis for the use of electronic evidence. Such a basis is already provided for in the ITE Law and reinforced by the 2025 Criminal Procedure Code. The unresolved issue is the standard for evaluating inferences derived from electronic evidence to prove *mens rea*. This gap creates broad discretion for judges while increasing reliance on expert testimony and the results of technical analyses.

Therefore, a doctrinal reconstruction is needed that organizes the proof of cyber *mens rea* into three distinct layers. First, digital evidence must meet the criteria of legality, authenticity, integrity, and relevance. Second, the methods used to derive technical or algorithmic inferences must be explainable, testable, and accountable. Third, the legal conclusion regarding *mens rea* must still be determined by the judge based on the totality of the evidence and the conviction reached through the system of proof under the law, applying the principle of negative presumption. This reconstruction harmonizes the Criminal Code (KUHP), the Criminal Procedure Code (KUHP), the Electronic Information and Transactions Law (UU ITE), and the Personal Data Protection Law (UU PDP) without altering the respective functions of each. Technology is thus positioned as a means to discover and process facts, while the determination of guilt remains a legal matter within the jurisdiction of the courts.

3.3 Constructing the Guilty Mind from Digital Traces: The Indra Kenz Judgment

The Tangerang District Court convicted Indra Kenz of two offences with very different evidentiary characters. The first was the dissemination of false and misleading news, causing consumer loss in electronic transactions; the second was money laundering. The factual core was an affiliate scheme around the Binomo binary-option application: through promotional videos, social-media posts, and direct messaging, the defendant projected an image of effortless

wealth and steered followers toward a platform on which, the court found, the great majority of participants were structurally bound to lose.³¹ The combination of these two charges is what makes the judgment a useful laboratory, because the *mens rea* of the speech offence and the *mens rea* of the laundering offence rest on different kinds of digital proof.

For the speech offence, the panel had to construct “with intent and without right.” It did so almost entirely by the indirect route. The court did not, and realistically could not, locate a single document in which the defendant confessed an intention to deceive consumers. Instead, it inferred the inner attitude from a mosaic of electronic materials, victim testimony, the promotional content itself, account and chat records, and the flow of funds through bank accounts, reading them together as evidence that the defendant knew the representations were false and willed the consequences. This is the classic structure of *willens en wetens* reconstructed from objective context: the deliberateness of the production, the targeting of an identified audience, and the defendant’s knowledge of how the promoted instrument worked were treated as sufficient to establish that the falsehood was intended rather than careless. In the vocabulary of comparative doctrine, this is close to inferring knowledge from *wilful blindness*, treating a person who deliberately avoids confirming an obvious truth as though they knew it.³²

For the laundering offence, the panel relied substantially on the Result of Analysis Report (*Laporan Hasil Analisis*) of the Financial Transaction Reports and Analysis Centre, which traced the movement of proceeds into assets and consumption.³³ Here the evidentiary character shifts from human testimony to institutional, partly algorithmic, analysis of transaction patterns. The report does not narrate the defendant’s state of mind; it reconstructs a pattern from which the court infers knowledge that the funds derived from crime. The same logic underlies the digital forensic extraction of devices and accounts, where tools of the Cellebrite type produce structured outputs, timelines, message threads, location data, whose interpretation the court must accept largely on the strength of the tool’s reputation rather than on a transparent account of how the output was generated. The point is not that the analysis is wrong. It is that the inference of intent now travels through artefacts the defence has limited means to test, which is exactly the structural concern that Pasquale’s pillars of disclosure, audit, and recourse are meant to address.

Read through Hildebrandt’s frame, the judgment poses a sharp question of subjecthood. The defendant remained a full legal subject only to the extent that he could meaningfully contest the construction placed upon his digital traces,³⁴ including the analytic report that helped ground the laundering conviction. Where the route to intent runs through an institutional or

³¹ Boby Agusty and Rahtami Susanti, “Perlindungan Hukum Korban Binary Option (Studi Kasus Indra Kenz),” *UMPurwokerto Law Review* 4, no. 2 SE-Articles (February 19, 2024): 299–308, <https://doi.org/10.30595/umplr.v4i2.16455>.

³² Panggalih Husodo et al., “Willful Blindness Sebagai *Mens rea* Telaah Filsafat Hukum H.L.A. HART,” *Qonun: Jurnal Hukum Islam Dan Perundang-Undangan* 9, no. 2 (2025): 163–90, <https://doi.org/10.21093/qj.v9i2.12130>.

³³ Wahyudi BR, “Pengaturan Hukum Pusat Pelaporan Dan Analisis Transaksi Keuangan (PPATK) Sebagai FIU (Financial Intelligence Unit) Di Indonesia,” *UNES Law Review* 6, no. 3 (2024): 9187–99, <https://doi.org/10.31933/unesrev.v6i3.1874>.

³⁴ Adji Saputra, Kristiawanto Kristiawanto, and Mohamad Ismed, “Rekonstruksi Penegakan Hukum Tindak Pidana Siber Di Indonesia,” *Seikat: Jurnal Ilmu Sosial, Politik Dan Hukum* 3, no. 1 (February 9, 2024): 63–70, <https://doi.org/10.55681/seikat.v3i1.1186>.

algorithmic output, the practical capacity to challenge that output, to interrogate its method, its assumptions, and its error rate, becomes the difference between a defendant who is tried and a defendant who is processed. In the Indra Kenz proceedings, the evidence was abundant, and the conviction was upheld on appeal, on cassation, and against a petition for review, so the outcome itself is not in doubt. The instructive feature is the method, an intent built by inference from machine-mediated material, because that method will be repeated in cases where the evidence is thinner, and the stakes for the presumption of innocence are higher.

In connection with the above, the Tangerang District Court Decision Number 1240/Pid.Sus/2022/PN Tng is one of the important rulings in the development of cybercrime law in Indonesia because it shows how the court builds proof of *mens rea* almost entirely through electronic evidence. Unlike conventional crimes, where intent can generally be proven through physical actions or the perpetrator's confession, this case demonstrates that the subjective element is inferred through a series of digital traces that are then connected into one construction regarding the defendant's knowledge and will. Therefore, the analysis of the *ratio decidendi* of this decision is focused on the relationship between types of digital evidence, the inferences made by the judge, and the conclusion about *mens rea*.

The analysis of the ruling shows that the panel of judges used at least four proof indicators to establish the element of intent. First, digital content serves as an indicator of the defendant's knowledge. The panel assessed that the promotional videos, social media posts, and electronic communications created by the defendant were not just promotional materials, but showed an understanding of how the Binomo platform works. The judges felt that the consistent narrative about high profits, depiction of a luxurious lifestyle, and invitations to join couldn't be seen as neutral expressions, but rather as a series of actions indicating that the defendant knew the nature of the product they were promoting. So, the digital evidence wasn't used just to prove that content was published, but also to infer the defendant's level of knowledge about the consequences of publishing it.

Second, the pattern of digital communication as an indicator of intent. The panel did not find evidence explicitly showing the defendant's acknowledgment of a desire to mislead consumers. However, the judge drew inferences from the repetitive communication patterns, consistent promotional targets, and the continuity of the defendant's digital activities. These inferences indicate that the promotion was not done by chance, but as part of a deliberate strategy to encourage the public to use a certain platform. In this way, the element of "intentionality" is established through consistent digital behavior, not through direct admission.

Third, electronic transaction traces serve as indicators of the relationship between economic gains and digital activity. In proving money laundering crimes, judges give significant weight to the PPATK Analysis Report, which shows patterns of receiving, transferring, and using funds from Binomo affiliate activities. This evidence doesn't directly prove the defendant's state of mind, but it forms the basis for judges to conclude that the defendant knew the source of the funds they received. In this way, inferences about *mens rea* are built through the logical connection between financial transaction patterns and digital activities that were previously deemed illegal.

Fourth, the integration of various electronic evidence as the basis for overall inference. No single piece of evidence independently proves the element of intent. Instead, *mens rea* is built through the accumulation of various types of evidence, namely digital content, electronic communications, account activity history, witness statements, and financial transaction analysis. The panel's rationale shows that intent is understood as the result of synthesizing the entire series of digital facts (cumulative inference), not as a fact proven directly.

These four indicators show that the process of proving in this case is essentially an inferential process. The relationship between electronic evidence and *mens rea* is not direct, but is built through a judge's reasoning based on the connections between digital facts. This kind of proof model is still consistent with the legal theory of evidence in a negative sense as long as the inferences are based on legitimate evidence and evaluated rationally. However, the greater the reliance on digital inference, the more important transparency becomes regarding how these inferences are formed.

The problem comes up when some electronic evidence comes from technical analysis done by agencies or forensic software. The Analysis Reports from PPATK or the results of digital device extraction are basically analytical products built using certain methods. In court practice, judges usually accept these results as supporting evidence without deeply examining the assumptions, analysis models, or accuracy levels. As a result, there's a risk that technical inferences gradually turn into legal inferences about *mens rea*, even though the two are very different. This is where the concept of algorithmic accountability comes in, which is about making sure that the digital inference process remains explainable, auditable, and contestable by the defendant.

An analysis of the Indra Kenz ruling identifies three distinct layers that must be distinguished in proving cyber *mens rea*. The first layer consists of digital facts, that is, data or activities whose existence can be proven through electronic devices or systems. The second layer consists of technical inferences, that is, the results of processing or analyzing digital facts using specific methods. The third layer consists of legal conclusions, that is, the judge's assessment of whether the totality of the facts proves the knowledge, intent, or other forms of *culpability* required by criminal law.

These three layers highlight the core issue in proving cyber *mens rea*. The more complex the technology used to generate evidence, the greater the need to explain how digital facts are transformed into technical inferences and how those inferences are subsequently used in legal reasoning. Failing to distinguish between these three elements can result in technical findings being given greater weight than they should have.

Therefore, the *ratio decidendi* of the Tangerang District Court's decision is significant not only because it resulted in a conviction that has become final and binding. The analytical value of the decision lies in the way the panel established intent through the accumulation of digital evidence, communications, and financial transactions. This pattern demonstrates that proving *mens rea* in cybercrimes is fundamentally inferential. The normative evaluation that can be drawn from this decision is that such inferences must remain within the bounds of the judge's legal reasoning. Digital evidence can show what was done, when it was done, with whom it

was done, and how an activity unfolded; however, the determination of whether these facts prove that the defendant knew of and intended the criminal act must still be explained through a *ratio decidendi* that is subject to scrutiny.

3.4 Mathematical Determinism and the Illusion of Algorithmic Objectivity

If the inner attitude is hard to prove by conventional means, a tempting alternative is to let the data speak. Every digital movement leaves a trail: access logs, transaction histories, communication patterns, device metadata, and from these traces an algorithm is said to reconstruct a more accurate picture of what is in a person's mind than any human testimony could. This is the essence of mathematical determinism, the belief that human behaviour, including malicious intent, can ultimately be reduced to measurable, predictable, and mathematically provable computation. In the criminal field, it appears in three forms: predictive policing, which forecasts where and by whom an offence will occur; forensic big-data analysis, which builds narratives of suspect behaviour from massive datasets; and AI-based risk assessment, which scores a defendant's "dangerousness" for decisions on detention, trial, and sentence.³⁵

The best-known and most contested example of the third form is the Correctional Offender Management Profiling for Alternative Sanctions, or COMPAS, used across several United States jurisdictions.³⁶ The system produces a risk score from many variables, which judges then weigh in detention and sentencing decisions. In *State v. Loomis*, the Wisconsin Supreme Court held that consideration of a COMPAS score at sentencing did not violate due process,³⁷ even though the defendant could not learn how the score was calculated because the method was protected as a trade secret; the court did, however, require that such scores be accompanied by written warnings about their limits. The European Union has been more cautious: Article 22 of the General Data Protection Regulation gives individuals the right not to be subject to decisions based solely on automated processing,³⁸ and the Artificial Intelligence Act classifies AI systems used in law enforcement as high-risk and subjects them to strict oversight.³⁹

Comparable developments appear in Asia with different dynamics: China integrates large-scale behavioural data into judgments with legal implications,⁴⁰ while debates over predictive analytics and facial recognition intensify elsewhere in the region. But this is where the real danger surfaces, in the illusion of objectivity. An algorithm looks neutral because it works with

³⁵ Cynthia Ayu Windani, "Strategi Dan Tantangan Predictive Policing Di Era Big Data Bagi Masyarakat Modern," *Deviance Jurnal Kriminologi* 7, no. 2 (December 31, 2023): 101–20, <https://doi.org/10.36080/djk.2385>.

³⁶ Michael Mayowa Farayola et al., "Ethics and Trustworthiness of AI for Predicting the Risk of Recidivism: A Systematic Literature Review," *Information* 14, no. 8 (July 27, 2023): 426, <https://doi.org/10.3390/info14080426>.

³⁷ Ellora Israni, "Due Process Algoritma: Kesalahan Akuntabilitas Dan Atribusi Dalam Kasus *State v. Loomis*," *Harvard Journal of Law & Technology Digest (JOLT Digest)*, 2017, <https://jolt.law.harvard.edu/digest/algorithmic-due-process-mistaken-accountability-and-attribution-in-state-v-loomis-1>.

³⁸ Halefom Abraha, "Regulating Algorithmic Employment Decisions through Data Protection Law," *European Labour Law Journal* 14, no. 2 (June 2, 2023): 172–91, <https://doi.org/10.1177/20319525231167317>.

³⁹ J Nicholas Shumate et al., "Governing AI in Mental Health: 50-State Legislative Review," *JMIR Mental Health* 12 (October 31, 2025): e80739–e80739, <https://doi.org/10.2196/80739>.

⁴⁰ Davide Giacomo Zoppoloto and Paolo Davide Farah, "China's Path to Modernization and Legal Pluralism: Transplants and the Belt and Road Initiative," *Asian Journal of Law and Society* 12, no. 2 (June 17, 2025): 109–44, <https://doi.org/10.1017/als.2025.7>; Xuechen Chen and Lu Xu, "State, Society, and Market: Interpreting the Norms and Dynamics of China's AI Governance," *Computer Law & Security Review* 59 (November 2025): 106206, <https://doi.org/10.1016/j.clsr.2025.106206>.

numbers rather than visible human prejudice, yet every model is built on historical data, and historical data encodes historical injustice. If, for decades, certain groups were arrested and convicted more often because they were more heavily scrutinised rather than because they offended more, the data teach the model to reproduce the pattern, the familiar principle that biased input yields biased output, however sophisticated the architecture.

A 2016 investigation found that COMPAS rated Black defendants nearly twice as likely to reoffend as white defendants even when other variables were controlled,⁴¹ so that the celebrated mathematical objectivity turned out to be old discrimination dressed in new statistical notation, and harder to challenge for wearing the costume of science. Pasquale names the underlying structure the black box,⁴² a system whose inputs and outputs can be observed but whose internal process cannot be traced,⁴³ and he argues that any computational system used in high-stakes domains must satisfy three demands: disclosure, so that the system can be opened and explained to those it affects; audit, so that its operation can be independently verified by competent experts; and recourse, so that those it burdens have an effective means of contesting its decisions. To these he adds, in his later work, four “new laws of robotics,” the first of which is squarely relevant to adjudication: artificial intelligence must complement, not replace, the human professional, which in this setting forbids the substitution of the judge’s reasoned conviction by an algorithmic score.⁴⁴

It is here that mathematical determinism collides with the basic logic of criminal justice. Criminal law punishes an individual for what they did and for their intent, not for what is statistically likely of people who share their profile. When an algorithm replaces the assessment of *mens rea* with probabilistic calculation, the operation quietly shifts from condemning a crime to condemning a potential crime, a logic closer to preemption than to justice.

In the Indonesian criminal justice system, transparency means the availability of sufficient information regarding the sources of data and the methodology of the analysis relevant to understanding the results presented as evidence. Auditability means that the methods and results of the analysis can be examined by competent parties. Contestability means that the defendant is given an effective opportunity to challenge and refute those results. These three principles do not constitute a new form of evidence, but serve as standards for assessing the quality and verifiability of electronic evidence or analysis results that have been lawfully obtained.

This connection is crucial in Indonesia’s criminal evidentiary system. The admissibility of electronic evidence does not mean that every result of electronic processing carries the same

⁴¹ Tim R  z, “Understanding Risk with FOTRES?,” *AI and Ethics* 3, no. 4 (November 6, 2023): 1153–67, <https://doi.org/10.1007/s43681-022-00223-y>; Francesca Lagioia, Riccardo Rovatti, and Giovanni Sartor, “Algorithmic Fairness through Group Parities? The Case of COMPAS-SAPMOC,” *AI & Society* 38, no. 2 (April 28, 2023): 459–78, <https://doi.org/10.1007/s00146-022-01441-y>.

⁴² Margaret Hu, “Cambridge Analytica’s Black Box,” *Big Data & Society* 7, no. 2 (July 24, 2020), <https://doi.org/10.1177/2053951720938091>.

⁴³ Meike Nauta et al., “From Anecdotal Evidence to Quantitative Evaluation Methods: A Systematic Review on Evaluating Explainable AI,” *ACM Computing Surveys* 55, no. 13s (December 31, 2023): 1–42, <https://doi.org/10.1145/3583558>.

⁴⁴ Frank Pasquale, “The New Laws of Robotics,” Brooklyn Law School, 2021, <https://lawnotes.brooklaw.edu/issue/spring-2021/the-new-laws-of-robotics/>.

probative value. Electronic evidence must still be evaluated based on the validity of its acquisition, its relevance, its integrity, and its logical connection to the elements of the criminal offense that must be proven. These conditions become even more critical when electronic evidence has undergone extraction or analysis using specific software. It is not enough for a judge to simply know that a piece of software has produced a conclusion. The judge needs to know what facts were analyzed, how the data was obtained, what methods were used, and whether the results can be verified and tested by the defense.

The relationship between algorithm-based decision-making and Indonesian criminal procedures can be divided into three stages. During the investigative stage, algorithmic analysis can be used to identify, categorize, and link digital data relevant to an alleged criminal offense. This function is investigative in nature and must not be treated as a conclusion regarding a person's guilt. The results of the analysis at this stage should be used to guide the search for other evidence. During the prosecution phase, the results of algorithmic analysis must be translated into concrete evidentiary connections. The prosecutor must demonstrate how the digital facts obtained relate to the elements of the crime and why those facts support a conclusion regarding *mens rea*. During the trial phase, the judge must conduct an independent assessment of the validity, reliability, relevance, and probative value of the analysis results and evaluate them in conjunction with other evidence.

This framework demonstrates that comparative experiences are not presented as legal models that Indonesia must adopt, but rather as a basis for defining the limits of technology use in national criminal procedures. *State v. Loomis* illustrates the importance of restricting the use of algorithmic scores and judicial oversight. The GDPR and the Artificial Intelligence Act establish principles regarding human oversight, transparency, and control over high-risk systems. Pasquale's ideas regarding transparency, auditability, and contestability provide a conceptual framework to ensure that computational results can be challenged by affected parties. These three experiences can be synthesized into Indonesia's legal requirements, which include testing the legality, reliability, and relevance of the results, ensuring the clarity of the methodology, and providing the opportunity to challenge the results of the analysis.

This synthesis also clarifies the boundary between algorithmic results and the proof of *mens rea*. Algorithmic results can support a judge's assessment if the data used is relevant to the case, obtained through lawful procedures, its integrity can be verified, the analysis method is accountable, and the defendant has had an adequate opportunity to challenge it. These results must also be supported by other evidence demonstrating a connection between the defendant's digital activities and their mental state. Conversely, algorithmic results cannot serve as the sole basis for concluding intent if they merely indicate probability, pattern similarities, or the possibility of criminal behavior.

This approach has practical implications for the assessment of *mens rea*. The fact that the defendant engaged in certain transactions, communicated with certain parties, used certain devices, or exhibited certain patterns of digital activity are facts that can be evaluated during the trial. Algorithms can help identify connections among these facts. Determining whether such connections indicate that the defendant knew of and intended the alleged acts remains a legal matter. Judges cannot delegate this assessment to software because algorithms lack the

authority to determine whether the elements of criminal liability under criminal law have been met.

Thus, comparative experience actually reinforces the need to adapt the use of technology to the structure of Indonesia's criminal procedures. Technology can serve as a tool for obtaining and processing information, while evidentiary procedures remain the mechanism for testing that information. Algorithmic results can strengthen the construction of evidence if they meet standards of legality, reliability, relevance, transparency, auditability, and contestability. The assessment of *mens rea* must still be conducted by a judge based on the totality of admissible evidence. This approach allows Indonesian law to leverage the analytical capabilities of technology without turning algorithms into decision-makers in criminal cases.

3.5 The Structural Tension with the Presumption of Innocence

There is something fundamental in the way modern criminal law regards a person standing before a court. He arrives not as a defendant who must prove his innocence, but as a human being presumed innocent until the state proves otherwise beyond a reasonable doubt. The presumption of innocence is not a procedural technicality; it is a civilisational statement about how state power must be limited when it confronts individual freedom,⁴⁵ and it was born from the Inquisition, from courts without defence, from systems that punished first and proved later. Mathematical determinism undermines that principle from within, often without anyone intending it to.

The deepest problem lies in the working logic of the risk-assessment algorithm. When a system rates a person's likelihood of offending from their digital behaviour, it does not prove that the person has committed a crime; it states that the person is likely to, or that their digital profile resembles that of past offenders. That is not proof in the legal sense; it is probability-based stigmatisation, and when such stigmatisation grounds harsher detention or sentence, the presumption of innocence is not merely interrupted but reversed. The reversal shows in a subtle shift in the burden of proof. In a healthy system, the state must prove guilt; once a machine has issued its probabilistic verdict, the defendant must refute the machine, and refuting a machine is harder than refuting a person. A witness can be confronted, their credibility tested, their account compared with other evidence; an algorithm working behind proprietary code, trained on inaccessible data, and producing a score without an intelligible explanation offers no comparable purchase.

Does the Indonesian system have enough defences against this risk? Some, but not enough. The procedural codes contain genuine protections. The old Code placed no burden of proof on the suspect or defendant, a direct codification of the presumption of innocence, and KUHAP 2025 carries the protective logic forward, requiring at least two lawful items of evidence both for the designation of a suspect and for conviction, and adding the exclusionary rule of Article 235 paragraph (5). Yet none of these provisions addresses the position of an algorithmic output as evidence, the transparency standards an analytic system must meet, or the defendant's right

⁴⁵ Adam Ilyas and Maman Sudirman, "Regulating Suspect Display in Press Conferences: Safeguarding Human Rights and The Presumption of Innocence," *Al-Adl : Jurnal Hukum* 17, no. 2 (July 27, 2025): 104–26, <https://doi.org/10.31602/al-adl.v17i2.19219>.

to access and contest the computation used to incriminate them. The Electronic Information and Transactions Law, revised more than once, is similarly silent on the standing of algorithmic output, and the National Criminal Code, while it now anchors fault in Article 36, does not anticipate that the “evidence” of intent might one day be a machine-generated score.

The contrast with other systems is instructive. The European Union already has an Artificial Intelligence Act with a strict risk classification, and the United States has, at least, a substantial jurisprudential debate through cases such as *Loomis*,⁴⁶ whereas Indonesia has no legal framework that expressly governs how, when, and on what conditions algorithmic systems may be used in criminal proceedings. The Circular Letter of the Minister of Communication and Informatics Number 9 of 2023 on the Ethics of Artificial Intelligence is a non-binding soft-law instrument, general in scope and without sanctions, and does not reach the criminal dimension. Hildebrandt’s answer to this danger is twofold and worth adopting. First, the right not to be subject to a decision based solely on automated processing, recognised in Article 22 of the GDPR and, for Indonesia, in Article 10 of the Personal Data Protection Law, should be read as a substantive shield in the criminal process, not merely a data-protection nicety. Second, legal protection should be built into the architecture of forensic and analytic systems by design, embedded at the stage of construction rather than appended after the system is already shaping a verdict.

A closer look at the evidentiary chain in the Indra Kenz proceedings exposes how much epistemic weight came to rest on instruments the defence could not meaningfully test. The chat logs, transaction records, and device extractions that anchored the finding of intent were not raw facts but the processed outputs of forensic and analytic tools, each carrying its own assumptions about relevance, completeness, and reliability. A mobile-forensic report does not simply reproduce a phone; it reconstructs it through proprietary parsing and carving routines whose error rates and design choices are rarely disclosed in open court. When such an artefact is presented as a faithful window into the defendant’s mind, the court is invited to treat an engineering product as if it were direct testimony. The accused, lacking access to the underlying methodology, is left to contest a conclusion rather than the process that produced it. That asymmetry is precisely what the doctrine of *willful blindness* was designed to police, yet it can also be the vehicle through which the asymmetry deepens. Used carefully, the doctrine captures the genuinely *culpable* actor who deliberately avoids confirming what they strongly suspect; used loosely, it lets a court infer a guilty mind from the mere fact that harm flowed through a defendant’s accounts. The *Global-Tech* standard guards against loose usage by demanding a subjective belief in a high probability of wrongdoing coupled with deliberate avoidance, not negligence dressed up as knowledge. Transposed to the digital sphere, this means a court should ask whether the defendant actually understood the fraudulent character of the scheme and chose not to look closer, not merely whether a reasonable person ought to have known. The distinction is doctrinally modest but practically decisive, because it keeps the line between fault and misfortune from dissolving into the volume of data the prosecution can assemble.

⁴⁶ Niamh Kinchin, “‘Voiceless’: The Procedural Gap in Algorithmic Justice,” *International Journal of Law and Information Technology* 32 (June 1, 2024), <https://doi.org/10.1093/ijlit/eaee024>.

The tension between mathematical determinism and the presumption of innocence cannot, then, be dissolved by procedural fine-tuning. It touches a more fundamental question: whether a legal order is willing to let the probabilistic logic of machines stand in for the moral logic of law that has been built, painstakingly, over centuries. If it is not, the task is to design a normative architecture that lets technological capacity serve as proof without letting it govern judgment.

Based on this analysis, this study proposes four normative parameters as judicial standards for evaluating the use of algorithmic analysis results to establish *mens rea*. These four parameters determine when algorithmic results can validly support a judge's assessment and when such results cannot be given decisive probative value. Algorithmic results may be used as evidence if they are obtained through lawful procedures, derived from relevant and verifiable data, based on accountable methods, and subject to scrutiny by the parties to the case. Even if these requirements are met, algorithmic results do not constitute direct evidence of intent. Such results can only serve as part of a body of evidence that assists the judge in drawing inferences regarding the defendant's mental state.

First, the results of algorithmic analysis can only be used to support an assessment of *mens rea* if there is a relevant connection between the analyzed data and the act and mental state to be proven. During the preliminary investigation and criminal investigation phases, algorithmic analysis can be used to identify patterns in transactions, communications, device activity, or relationships between data that are relevant to the alleged criminal offense. These results can serve as a basis for advancing the investigation and seeking other evidence. Algorithmic results cannot be used to establish that a person has criminal intent simply because the system finds similarities in patterns with the behavior of previous perpetrators. Statistical correlations or similarities in profiles do not, in and of themselves, indicate the defendant's knowledge or intent. Such an assessment must be based on facts that have a strong direct or indirect connection to the alleged acts and mental state.

Second, algorithmic results can only be considered admissible evidence if the underlying methods and data can be tested for reliability, integrity, and relevance. During the prosecution phase, the prosecutor must be able to explain the data sources, how the data was obtained and maintained, the extraction methods, the analysis methods, and the limitations of the results obtained. The judge must distinguish between the digital data that is the subject of the examination and the conclusions generated by the software based on that data. This distinction is important because the fact that a device or system records certain activities does not automatically prove that the defendant knew of, intended, or aimed to commit those acts. If the methods used cannot be adequately explained, the integrity of the data cannot be verified, or the connection between the analysis results and the *mens rea* element cannot be demonstrated, such algorithmic results should not be used as the primary basis for concluding intent.

Third, algorithmic results must be considered within a body of mutually reinforcing evidence. The evidentiary system must not transform the probabilities generated by an algorithm into certainty regarding the defendant's guilt. The prosecutor remains obligated to prove the elements of the criminal offense based on admissible evidence, while the judge must form a conviction based on the totality of the evidence examined during the trial. The results of

algorithmic analysis can strengthen witness testimony, expert testimony, documents, electronic evidence, or other evidence if each piece of evidence points to interrelated facts. Conversely, algorithmic results cannot compensate for deficiencies in other evidence or be used to fill gaps in the proof regarding subjective elements. Thus, algorithms function as corroborative evidence, not as a substitute for proving *mens rea*.

Fourth, the defendant must be given an effective opportunity to challenge the methods, data, assumptions, and results of the algorithmic analysis used against him or her. This principle requires the prosecutor and the party presenting the evidence to provide sufficient information so that the defense can assess the reliability of the evidence. This scrutiny may include the method of data collection, data integrity, extraction methods, analysis parameters, error rates, system limitations, and the relationship between the analysis results and the conclusions presented. The judge then evaluates these objections before determining the probative value of the algorithmic results. If the defense does not have an adequate opportunity to challenge the methodological basis of an algorithmic result, the judge must exercise caution in assigning weight to that result, particularly if it serves as the primary basis for concluding that there was intent.

These four parameters can be formulated as a phased judicial review of algorithmic evidence. The first phase concerns legality and relevance—ensuring that the evidence was obtained lawfully and is related to the elements of the criminal offense to be proven. The second phase concerns integrity and reliability—examining the integrity of the data as well as the methods used to obtain and analyze it. The third stage is the clarity of inference, which involves assessing whether the conclusions drawn can truly link digital facts to the *mens rea* element, rather than merely indicating a correlation or possibility. The fourth stage is adversarial scrutiny, which ensures that the defendant has the opportunity to challenge the evidence, methods, and conclusions presented. Only when all four stages are met can algorithmic results be lawfully used to support the judge’s inference regarding intent.

The standard also draws a clear distinction between digital facts, algorithmic inferences, and legal conclusions. Digital facts are information obtained from electronic devices or systems through verifiable procedures. Algorithmic inferences are conclusions generated by processing those facts based on specific methods. Legal conclusions regarding *mens rea* are the judge’s assessment of the totality of the evidence to determine whether the element of guilt has been proven. These three layers cannot be treated as a single entity. Judges must reason for themselves regarding the relationship among the three. Algorithms can help identify patterns and relationships in data, but they do not have the authority to determine whether the defendant acted with intent within the meaning of criminal law.

The application of these standards is crucial in cases involving large volumes of digital evidence. In the Indra Kenz case, for example, communication logs, transaction records, and device extraction results can be used to establish a chain of facts regarding the defendant’s activities. The probative value does not lie in the software’s ability to draw conclusions regarding intent, but rather in the prosecutor’s ability to demonstrate that these facts—after their validity and reliability have been tested—have a sufficient connection to the defendant’s knowledge, intent, and purpose. The judge must then evaluate that connection in conjunction

with other evidence. This approach prevents a leap in reasoning from “the defendant engaged in certain digital activities” to “the defendant must have known and intended the criminal consequences of those activities.”

This framework also sets limits on the application of the doctrine of willful blindness. This doctrine may only be applied if the trial evidence demonstrates that the defendant was aware of a strong possibility regarding unlawful circumstances or acts and intentionally avoided making efforts to ascertain those circumstances. The existence of transaction patterns deemed suspicious, account ownership, or the defendant’s involvement in an electronic system is not, in and of itself, sufficient to prove willful blindness. Algorithmic results can help identify relevant patterns, but the judge must still find a factual basis demonstrating subjective awareness and deliberate avoidance.

Thus, algorithmic results may legitimately support a judicial assessment of *mens rea* provided that such results are obtained lawfully, the data is relevant, and its integrity is guaranteed, the analytical methods are accountable, the inferences have a rational connection to the elements of guilt, can be challenged by the defense, and are corroborated by other admissible evidence. Conversely, algorithmic results cannot replace a judge’s assessment if they merely indicate probabilities, statistical correlations, profile similarities, or predictions regarding the likelihood of criminal behavior. This distinction is crucial for maintaining the boundary between factual inferences and legal conclusions. Technology can help explain what occurs within electronic systems, but determining whether the defendant knew, intended, or willfully avoided knowledge of the criminal act remains a legal matter to be decided by the judge.

With this framework, the use of technology in criminal evidence need not be viewed as a threat to the presumption of innocence. Technology can be used to discover, process, and correlate digital information as long as its use remains within the bounds of legality, relevance, reliability, admissibility, and judicial review. These limits ensure that computational capacity is used to strengthen the evidentiary process, not to replace the state’s obligation to prove the defendant’s guilt. These judicial standards ultimately position algorithms as epistemic instruments in the evidentiary process, while the determination of *mens rea* remains a judicial function of the judge based on the totality of admissible and verifiable evidence.

3.6 An Ontological Reconstruction of Cyber *Mens Rea*

Faced with the crisis sketched above, the two simplest responses are both wrong. The first is juridical nostalgia, rigidly preserving the classical doctrine as though the digital world did not exist; it is comfortable because it spares the labour of rethinking, but it fails in practice, for when a court is forced to use a nineteenth-century concept of intent to judge an attack executed by an autonomous system, the result is not justice but a legal fiction imposed on a reality its framers never imagined. The second is algorithmic capitulation, surrendering the assessment of intent to computation in the name of efficiency and objectivity; its dangers are documented above: a pseudo-objectivity that conceals bias, reverses the burden of proof, and turns criminal law into a more sophisticated but not more just sentencing machine. What is needed is neither, but a reconstruction of the cyber *mens rea* framework, honestly built on the recognition that

digital reality demands new legal categories, while remaining rooted in the values that make criminal law worthy of the name.

The reconstruction begins from a modest epistemological admission: *mens rea* need not always be proven by confession or by penetrating the offender's mind. The common law has long accepted, through the doctrines of constructive knowledge and *wilful blindness*, that intent may be inferred from the objective context of the act, so that a person who deliberately turns away from facts they ought to know may be treated as though they knew them.⁴⁷ On that bridge, this article proposes a three-layer framework. The first layer preserves subjective intention as the core, the offender's actual awareness of the nature of the act and its likely consequences, but adapts the standard of proof to digital reality: intent may be deduced from specific technical preparatory steps, the selection of identified targets, and knowledge of how the tools used operate.

The second layer is the objective technical context, the character of the system or tool used, the degree of automation involved, and the extent to which a human actor retained meaningful control over the course of the conduct; the higher the automation and the longer the causal chain, the heavier the demand to prove that the offender consciously designed or activated the mechanism. The third layer is normative proportionality, the principle that the weight of the proof demanded must be proportionate to how far an AI or automated system has displaced the human from the decision. Where the human remained the primary decision-maker, the classical standard applies in full; where the system made the operational decisions, responsibility shifted toward accountability for the design, deployment, and oversight of the system. Applied to the Indra Kenz judgment, the framework would have required the court to make explicit which layer carried the inference of intent, the deliberate human production of the promotional scheme on the speech count, and the institutional analysis of transaction patterns on the laundering count, and to subject the latter to a transparency it was not, on the face of the practice, required to meet.

The framework has comparative precedent. The United Kingdom, through the Computer Misuse Act 1990 as amended, developed the concept of an intent to impair the operation of a computer in general,⁴⁸ a flexible adaptation of *mens rea* that does not require intent toward a specific victim yet keeps a subjective element. Germany, within the *Strafgesetzbuch*,⁴⁹ allows intent to be proven through conscious acceptance of risk under the doctrine of *dolus eventualis*, which fits cybercrime where the offender may not desire a specific consequence yet consciously accepts its possibility. Singapore, through its revised Computer Misuse Act, introduced a gradation of *mens rea* from knowing to reckless, giving the prosecutor flexibility to fit the charge to the technical complexity of the offence.

The framework also dovetails with the paradigm shift of the National Criminal Code. The Code moves from a rigidly retributive model toward an individualised one, giving judges explicit

⁴⁷ Husodo et al., "Willful Blindness Sebagai *Mens rea* Telaah Filsafat Hukum H.L.A. HART."

⁴⁸ Maria Minerva Gani et al., "Cyber Law Awareness Regarding Illegal Access and Data Breaches in Indonesia," *JIHAD: Jurnal Ilmu Hukum Dan Administrasi* 8, no. 1 (2026): 190–202, <https://doi.org/10.58258/jihad.v8i1.10468>.

⁴⁹ Hafita Mutiara Zaharani, "Tinjauan Yuridis Pengaturan Pidana Pokok Dan Tujuan Pemidanaan Dalam KUHP 2023 Indonesia Dan Strafgesetzbuch Jerman," *Depositi: Jurnal Publikasi Ilmu Hukum* 3, no. 2 (June 4, 2025): 47–58, <https://doi.org/10.59581/deposisi.v3i2.5064>.

sentencing guidelines (*pedoman pemidanaan*) and stating the purposes of punishment in Articles 51 and 52, which include the restoration of balance and which forbid sentencing that degrades human dignity.⁵⁰ Under these guidelines, the judge must weigh not only the objective harm but the offender's motive, inner state, and actual degree of *culpability*, and the three-layer framework gives the judge a doctrinal instrument to calibrate that *culpability* when an algorithm or autonomous system mediated the offence, keeping faith with the maxim *geen straf zonder schuld*, no punishment without fault, so that the sanction tracks the human actor's genuine control rather than the arbitrary scale of automated damage. Where a system departs significantly from its human-assigned parameters to cause unforeseen harm, proportionality may counsel shifting the focus, for instance, from individual imprisonment toward corporate accountability or restorative measures, within the double-track logic the Code now embraces.

None of this works, however, unless the machine-mediated material on which intent is built can itself be tested. Pasquale's three pillars supply the missing procedural layer. Disclosure would require that the method of a forensic extraction or a financial-intelligence analysis be explained, in substance, to the defence rather than shielded as a trade secret. An audit would allow an independent, competent expert to verify how a tool of the Cellebrite type, or the analytic process behind a Result of Analysis Report, produced its output. Recourse would guarantee the defendant a real opportunity to contest that output before it hardens into a finding of intent. Read together with Pasquale's first new law of robotics, that AI must complement rather than replace the human professional, these pillars keep the judge's reasoned conviction, and not the machine's score, as the operative ground of decision.

For Indonesia, the comparative and theoretical lessons converge on a reform agenda that is *ius constituendum* in the proper sense, law as it ought to be. The agenda has three parts. The first is the codification of an adjusted standard for proving *mens rea* in cyber offences, whether through revision of the Criminal Code or through implementing regulations of the Electronic Information and Transactions Law, so that the translation of a digital pattern into *willens en wetens* no longer rests on unguided discretion. The second is a regulatory framework governing the use of AI and forensic-analytic systems in criminal enforcement, setting obligations of algorithmic transparency and a defendant's right to contest system outputs, filling the space that the non-binding Circular Letter Number 9 of 2023 on the Ethics of Artificial Intelligence leaves open. The third is the strengthening of the technical capacity of investigators, prosecutors, and judges, so that the assessment of intent is not trapped in a formalism that loses its substance. Pursued together, these measures would let Indonesian jurisprudence remain technologically literate without ceasing to be humane.

Operationalising meaningful human control⁵¹ in the proof of cyber *mens rea* requires more than a slogan; it requires allocating concrete duties at each point where a machine output enters the chain of reasoning toward guilt. At the investigative stage, it means that a forensic analyst must be able to explain, in terms a court and a defendant can interrogate, what a tool measured, what

⁵⁰ Mochamad Januar Rizki, "Mengenal Konsep Baru Jenis Pemidanaan Dalam KUHP Nasional," Hukumonline, 2024, <https://www.hukumonline.com/berita/a/mengenal-konsep-baru-jenis-pemidanaan-dalam-kuhp-nasional-lt662de997a2036/>.

⁵¹ Basya Radyananda, Faisal Abdaud, and Gamlan Dagani, "Analisis Limitasi Pertanggungjawaban Pidana Dalam Kejahatan Manipulasi Digital Di Indonesia," *Nomos: Jurnal Penelitian Ilmu Hukum* 6, no. 1 (2026): 1–7, <https://doi.org/10.56393/nomos.v6i1.4273>.

it inferred, and where its margins of error lie. At the prosecutorial stage, it means that the inference from a digital trace to a state of mind must be argued openly rather than smuggled in under the authority of the instrument that produced the trace. At the adjudicative stage, it means that a judge retains, and is seen to retain, the final responsibility for the attribution of fault, refusing to defer to a number simply because it is precise. Human control, in this sense, is not nostalgia for a pre-digital courtroom; it is the procedural expression of the principle that *culpability* is a normative judgment about a person, not a statistical property of a dataset.

None of this will work without institutional capacity to match the ambition. A right to contest an automated inference is hollow if the defence bar, the prosecution, and the bench lack the technical literacy to exercise and assess it, and if courts lack access to independent expertise capable of auditing the tools on which prosecutions increasingly rely. Indonesia's adoption of the National Criminal Code and the new Criminal Procedure Code therefore needs to be accompanied by sustained investment in judicial training, in publicly accountable forensic standards, and in mechanisms through which the reliability of investigative software can be examined without surrendering wholesale to claims of trade secrecy. The *Loomis* experience is a warning here: a court may permit the use of an opaque tool while issuing cautionary instructions, but a caution that the decision-maker cannot fully understand offers thin protection. Building the capacity to look inside the black box is, in the end, inseparable from the doctrinal reform the digital age demands.

The application of this framework can be illustrated through the Tangerang District Court Decision Number 1240/Pid.Sus/2022/PN Tng in the Indra Kenz case. At the first level, the element of intent was proven through the defendant's conscious actions in producing promotional content, communicating with potential investors, and earning profits from affiliate activities. At the second level, evidence such as transaction logs, electronic communications, and PPATK analysis results were used to show the link between digital activities and the flow of proceeds from the crime. However, at the third level, this study found that the court had not explicitly tested the reliability of the digital analysis methods used to build those inferences. As a result, the connection between electronic evidence and the conclusion regarding *mens rea* still heavily relies on assumptions about the validity of the analytical tools used.

This three-layered framework also puts the concept of meaningful human control into practice. At every stage of proof, the final decision about the existence of *mens rea* must remain with the judge. Forensic software, transaction analysis systems, or artificial intelligence only serve as supporting tools to identify technical facts, not as legal decision-makers. So, assessing intent still remains a normative judgment made by humans based on all the evidence available.

This model also incorporates the three main principles of algorithmic accountability as developed by Pasquale, namely transparency, auditability, and contestability. Transparency requires that digital analysis methods can be explained to the court; auditability allows for independent testing of the reliability of forensic software; while contestability ensures the defendant's right to challenge and refute the digital inferences used against them. These three principles are prerequisites to ensure that the use of technology remains in line with the presumption of innocence and the principle of a fair trial.

The practical implications of this framework differ for each law enforcement actor. For investigators, it requires thorough documentation of digital forensic methods so that the chain of evidence can be verified in court. For prosecutors, it mandates a clear separation between digital facts, technical interpretations, and arguments about intent, so that charges don't rely solely on algorithmic analysis results. For judges, it provides a more systematic way to assess whether inferences about *mens rea* are genuinely supported by valid evidence or have shifted into a reversal of the burden of proof. Meanwhile, for policymakers, it offers a conceptual basis for creating standards on the use of artificial intelligence and analytical systems in criminal justice processes.

On that basis, this study proposes three *ius constituendum* agendas. First, the drafting of normative standards regarding the proof of *mens rea* in cybercrime, which regulate the indicators of inference that are acceptable to the court. Second, the establishment of regulations regarding the use of artificial intelligence systems and analytical tools in criminal proceedings, requiring transparency, independent audits, and the defendant's right to challenge the analysis results. Third, enhancing the technical capacity of investigators, prosecutors, judges, and digital forensic experts so they can critically evaluate the reliability of electronic evidence.

These four parameters form a multi-layered relationship within the evidentiary process. During the investigation and inquiry stages, the first parameter limits the algorithm's function to that of a tool for searching and processing information. During the prosecution stage, the second parameter requires the prosecutor to establish a connection between the results of the digital analysis and the body of admissible evidence as a whole. During the evidence examination and evaluation stage, the third parameter requires that the methods used be technically and legally justifiable. During the defense and judicial deliberation stages, the fourth parameter ensures that the defendant has the opportunity to challenge the evidence and the methods used against them. With this framework, the assessment of *mens rea* remains the judge's prerogative and is not delegated to an algorithmic system.

This model also provides a clearer distinction between digital facts, algorithmic inferences, and legal conclusions. Digital facts are information obtained from electronic devices or systems through accountable procedures. Algorithmic inferences are conclusions generated by processing these facts based on specific methods. Legal conclusions regarding *mens rea* are the judge's assessment of the totality of the evidence to determine whether the element of *culpability* has been proven. These three layers should not be treated as a single entity. Algorithmic results can strengthen the evidentiary process, but they cannot replace a legal assessment of intent.

Thus, the tension between algorithmic inference and the presumption of innocence is not a reason to reject the use of technology in criminal evidence. Rather, this challenge highlights the need for a normative framework that defines the limits of technology's role at every stage of the criminal process. Technology can help the state discover, process, and link digital information, but the authority to determine whether the elements of a crime have been met remains with law enforcement officials and judges based on evidence that is admissible, verifiable, and rationally assessable. This approach ensures that the use of electronic evidence

remains consistent with due process of law, equality of arms, and the presumption of innocence as the foundations of the rule of law.

4. CONCLUSION

This study concludes that proving mens rea in Indonesian cybercrime cases has fundamentally shifted from direct evidence of physical conduct toward inferential reconstruction based on digital traces, electronic communications, transaction records, and forensic or algorithmic analysis. The analysis of the Indonesian evidentiary framework and Tangerang District Court Decision No. 1240/Pid.Sus/2022/PN Tng demonstrates that, although electronic evidence is legally recognized, Indonesian law does not yet provide sufficiently explicit standards for distinguishing the evidentiary status of digital facts, technical or algorithmic inferences, and legal conclusions concerning mens rea. The principal novelty of this study is the formulation of a three-layer cyber mens rea framework that integrates subjective criminal intent with the technical characteristics of digital evidence and the normative requirements of algorithmic accountability. Under this framework, digital facts must satisfy legality, authenticity, integrity, and relevance; technical or algorithmic inferences must be transparent, explainable, auditable, and open to effective challenge; and the ultimate determination of mens rea must remain within judicial reasoning based on the totality of admissible evidence. This reconstruction clarifies the respective functions of technology and legal judgment while preventing algorithmic outputs from becoming substitutes for judicial assessment. Accordingly, Indonesian criminal justice reform should establish explicit standards for algorithmic evidence, strengthen judicial guidelines for evaluating digital inferences, and guarantee meaningful defence access to the methods underlying computational evidence, thereby safeguarding the presumption of innocence and due process.

REFERENCES

- Abraha, Halefom. "Regulating Algorithmic Employment Decisions through Data Protection Law." *European Labour Law Journal* 14, no. 2 (June 2, 2023): 172–91. <https://doi.org/10.1177/20319525231167317>.
- Aditia, Ahmad Bagus, and Muchamad Iksan. "The Relevance of Judicial Beliefs in the Negative Proof System of Article 183 of the Criminal Procedure Code: Analysis of Surabaya District Court Decision Number 454/Pid.B/2024/Pn.Sby." *Academia Open* 10, no. 2 (December 12, 2025). <https://doi.org/10.21070/acopen.10.2025.12995>.
- Agatha, Claudia, and R. Rahaditya. "Fragmented Digital Forensic Standards in Indonesian Criminal Evidence." *Indonesian Journal of Law and Economics Review* 21, no. 2 (May 20, 2026): 1–11. <https://doi.org/10.21070/ijler.v21i2.1558>.
- Agusty, Bobby, and Rahtami Susanti. "Perlindungan Hukum Korban Binary Option (Studi Kasus Indra Kenz)." *UMPurwokerto Law Review* 4, no. 2 SE-Articles (February 19, 2024): 299–308. <https://doi.org/10.30595/umplr.v4i2.16455>.
- Alexander, Ariel, Boy Gabriel Yohanes Simarmata, Dyo Ganda Siadari, Michelle Evelyn Marpaung, and Patrisia Tanwijaya. "Analisis Yuridis Kekuatan Pembuktian Dalam Putusan Pengadilan Negeri Praya." *Syntax Literate ; Jurnal Ilmiah Indonesia* 10, no. 10 (October 4, 2025): 8262–75. <https://doi.org/10.36418/syntax-literate.v10i10.61788>.
- Aljundani, Arifuddin, and Niru Anita Sinaga. "Penegakan Hukum Terhadap Pelaku Tindak Pidana Siber Tentang Akses Ilegal Di Indonesia." *Lex Laguens: Jurnal Kajian Hukum Dan Keadilan* 3, no. 2 (2025): 176–93. <https://doi.org/10.08221/lexlaguens.v3i2.271>.
- Ar, Aris Munandar, Wirda Wirda, Aditya Slamet Rusbandi, Muhammad Zulhendra, Saiful

- Bahri, and Danang Fajri. "Peran Niat (*Mens rea*) Dalam Pertanggungjawaban Pidana Di Indonesia." *Jimmi: Jurnal Ilmiah Mahasiswa Multidisiplin* 1, no. 3 (October 27, 2024): 240–52. <https://doi.org/10.71153/jimmi.v1i3.140>.
- Aziz, Abdul. "Rekonstruksi Hukum Penyalahgunaan Artificial Intelligence (AI) Dalam Konten Kesusilaan Dan Pencemaran Nama Baik." *Jurnal Hukum Lex Generalis* 6, no. 7 (2026): 1–30. <https://doi.org/10.56370/jhlg.v6i7.3209>.
- Baris Erman, Ragip. "Perspective Chapter: Criminal Responsibility." In *Criminal Behavior - The Underlyings, and Contemporary Applications*. IntechOpen, 2023. <https://doi.org/10.5772/intechopen.1002345>.
- Begishev, Ildar, Mehrdad Rayejian Asli, Veronika Denisovich, Andrey Majorov, and Andrey Sergeyev. "Research of Artificial Intelligence as a Subject of Crime." Edited by I. Abdullayev, V. Kukhar, E. Akhmetshin, D. Bekjanov, and A. Carballo-Penela. *E3S Web of Conferences* 449 (November 16, 2023): 03004. <https://doi.org/10.1051/e3sconf/202344903004>.
- Blackstone, Sir William. *Commentaries on the Laws of England*. Oxford: Clarendon Press, 1976.
- BR, Wahyudi. "Pengaturan Hukum Pusat Pelaporan Dan Analisis Transaksi Keuangan (PPATK) Sebagai FIU (Financial Intelligence Unit) Di Indonesia." *UNES Law Review* 6, no. 3 (2024): 9187–99. <https://doi.org/10.31933/unesrev.v6i3.1874>.
- Candra, Muhammad, and Muhammad Ruhly Kesuma Dinata. "Penegakan Hukum Terhadap Tindak Pidana Penyebaran Berita Hoaks Melalui Media Sosial." *Arus Jurnal Sosial Dan Humaniora* 5, no. 2 (August 1, 2025): 1577–86. <https://doi.org/10.57250/ajsh.v5i2.1373>.
- Chen, Xuechen, and Lu Xu. "State, Society, and Market: Interpreting the Norms and Dynamics of China's AI Governance." *Computer Law & Security Review* 59 (November 2025): 106206. <https://doi.org/10.1016/j.clsr.2025.106206>.
- Commission European. "Counting as a Human Being in the Era of Computational Law (CoHuBiCoL)." CORDIS – Community Research and Development Information Service, January 1, 2019. <https://doi.org/10.3030/788734>.
- Cowan, Nelson, Nick I. Ahmed, Chenye Bao, Mackenzie N. Cissne, Ronald D. Yee-Flores, Roman M. Gutierrez, Braden Hayse, et al. "Theories of Consciousness from the Perspective of an Embedded Processes View." *Psychological Review* 132, no. 1 (January 2025): 76–106. <https://doi.org/10.1037/rev0000510>.
- Dian Rusmana, Numan Sofari Hafid, and Syahrul Anwar. "Analisis Delik *Culpa* Dan Pertanggungjawaban Pidana Atas Kelalaian Pejabat Negara Dalam Perkara Korupsi Melalui Studi Putusan 68/Pid.Sus-TPK/2025/PN Jkt Pst." *Mahkamah : Jurnal Riset Ilmu Hukum* 2, no. 4 (December 19, 2025): 127–51. <https://doi.org/10.62383/mahkamah.v2i4.1333>.
- Dmitrieva, A. A., and P. S. Pastukhov. "Concept of Electronic Evidence in Criminal Legal Procedure." *Journal of Digital Technologies and Law* 1, no. 1 (March 16, 2023): 270–95. <https://doi.org/10.21202/jdtl.2023.11>.
- Erawan, Yevi Mulyana, Novayandra Arinuridin, and Muhammad Dwi Yuliandy. "Tantangan Pembuktian Kejahatan Siber (Cybercrime) Dalam Peradilan Pidana." *Al-Zayn : Jurnal Ilmu Sosial & Hukum* 4, no. 2 (2026): 3069–75. <https://doi.org/10.61104/alz.v4i2.4828>.
- Fadhila, Kharisma Wulan. "Reformasi Hukum Pidana Dan Pertanggungjawaban Korporasi Dalam UU KUHP 2023." *Action Research Literate* 8, no. 3 (March 25, 2024): 649–57. <https://doi.org/10.46799/ar.v8i3.277>.
- Farayola, Michael Mayowa, Irina Tal, Regina Connolly, Takfarinas Saber, and Malika Bendeache. "Ethics and Trustworthiness of AI for Predicting the Risk of Recidivism: A Systematic Literature Review." *Information* 14, no. 8 (July 27, 2023): 426. <https://doi.org/10.3390/info14080426>.

- Fransisco, Wawan. "Drafting Laws for The Lifeless: A Legal Framework for Criminal Liability and Punishment for Artificial Intelligence." *Jurnal Hukum Dan Peradilan* 14, no. 3 (November 30, 2025): 701–18. <https://doi.org/10.25216/jhp.14.3.2025.701-718>.
- Galih Orlando. "Hukum Sebagai Kontrol Sosial Dan Social Engineering." *Tarbiyah Bil Qalam : Jurnal Pendidikan Agama Dan Sains* 7, no. 1 (July 15, 2023). <https://doi.org/10.58822/tbq.v7i1.111>.
- Gani, Maria Minerva, Cheryl Nathania, Putra Dirgantara, Heigel Ritonga, Rifaldo Aditya, Nicole Yuri, Tasya Amira, Natasha Jhonray, and Yuni Priskila Ginting. "Cyber Law Awareness Regarding Illegal Access and Data Breaches in Indonesia." *JIHAD : Jurnal Ilmu Hukum Dan Administrasi* 8, no. 1 (2026): 190–202. <https://doi.org/10.58258/jihad.v8i1.10468>.
- Gelgi, Metehan, Yueting Guan, Sanjay Arunachala, Maddi Samba Siva Rao, and Nicola Dragoni. "Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques." *Sensors* 24, no. 11 (June 1, 2024): 3571. <https://doi.org/10.3390/s24113571>.
- Hafita Mutiara Zaharani. "Tinjauan Yuridis Pengaturan Pidana Pokok Dan Tujuan Pemidanaan Dalam KUHP 2023 Indonesia Dan Strafgesetzbuch Jerman." *Deposisi: Jurnal Publikasi Ilmu Hukum* 3, no. 2 (June 4, 2025): 47–58. <https://doi.org/10.59581/deposisi.v3i2.5064>.
- Hall, Jerome. *General Principles of Criminal Law*. Indianapolis: Bobbs-Merrill., 1960.
- Heriani, Fitri Novia. "Menakar Pertanggungjawaban Hukum Penggunaan Artificial Intelligence." *Hukumonline*, 2026. <https://www.hukumonline.com/berita/a/menakar-pertanggungjawaban-hukum-penggunaan-artificial-intelligence-lt69dcd592de37e/>.
- Hu, Margaret. "Cambridge Analytica's Black Box." *Big Data & Society* 7, no. 2 (July 24, 2020). <https://doi.org/10.1177/2053951720938091>.
- Husodo, Panggalih, Lisa Anggraini, Nurul Amin, and Elviandri Elviandri. "Willful Blindness Sebagai *Mens rea* Telaah Filsafat Hukum H.L.A. HART." *Qonun: Jurnal Hukum Islam Dan Perundang-Undangan* 9, no. 2 (2025): 163–90. <https://doi.org/10.21093/qj.v9i2.12130>.
- Ilyas, Adam, and Maman Sudirman. "Regulating Suspect Display in Press Conferences: Safeguarding Human Rights and The Presumption of Innocence." *Al-Adl : Jurnal Hukum* 17, no. 2 (July 27, 2025): 104–26. <https://doi.org/10.31602/al-adl.v17i2.19219>.
- Israni, Ellora. "Due Process Algoritma: Kesalahan Akuntabilitas Dan Atribusi Dalam Kasus State v. Loomis." *Harvard Journal of Law & Technology Digest (JOLT Digest)*, 2017. <https://jolt.law.harvard.edu/digest/algorithmic-due-process-mistaken-accountability-and-attribution-in-state-v-loomis-1>.
- Karo Karo, Rizky, and Teguh Prasetyo. "The Provision of Licensed Financial Technology Lending From The Perspective of Cyber Law and Criminal Law in Indonesia." *Pena Justisia: Media Komunikasi Dan Kajian Hukum* 24, no. 1 (September 30, 2025): 7263–80. <https://doi.org/10.31941/pj.v24i2.6559>.
- Kinchin, Niamh. "'Voiceless': The Procedural Gap in Algorithmic Justice." *International Journal of Law and Information Technology* 32 (June 1, 2024). <https://doi.org/10.1093/ijlit/eaee024>.
- Lagioia, Francesca, Riccardo Rovatti, and Giovanni Sartor. "Algorithmic Fairness through Group Parities? The Case of COMPAS-SAPMOC." *AI & Society* 38, no. 2 (April 28, 2023): 459–78. <https://doi.org/10.1007/s00146-022-01441-y>.
- Lagus, Wegestin, Salma Salma, and Bakhtiar Bakhtiar. "The Dynamics of Social Institutions in Family Law: Understanding Values, Norms, and Their Functions." *Al-Qanun: Jurnal Kajian Sosial Dan Hukum Islam* 6, no. 2 (October 2, 2025): 120. <https://doi.org/10.58836/al-qanun.v6i2.24685>.
- Mahmood, Abeer Abd Alhameed, and Wasan Hashim Al Masoody. "A Comprehensive

- Analysis of Botnet Detection and Distributed Denial of Service Attacks: The Function of Deep Learning and Machine Learning Methods.” *American Journal of Technology Advancement* 2, no. 2 (2025): 6–23. <https://doi.org/10.31150/ajta.v2i2.1089>.
- Mardiyati, Nursanti. “Keabsahan Hukum Fitur Pengaduan Shopee Sebagai Bukti Elektronik Dalam E-Commerce.” *Jurnal USM Law Review* 9, no. 1 (January 27, 2026): 50–74. <https://doi.org/10.26623/julr.v9i1.12896>.
- Nano, Vaulus Julianta, Tahasak Sahay, and Claudia Yuni Pramita. “Analisis Teoritis *Dolus* Dan *Culpa* Dalam Konsep Kesalahan Sebagai Dasar Pertanggungjawaban Pidana.” *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 4, no. 2 (2026): 6241–51. <https://doi.org/10.61104/alz.v4i2.5100>.
- Nauta, Meike, Jan Trienes, Shreyasi Pathak, Elisa Nguyen, Michelle Peters, Yasmin Schmitt, Jörg Schlötterer, Maurice van Keulen, and Christin Seifert. “From Anecdotal Evidence to Quantitative Evaluation Methods: A Systematic Review on Evaluating Explainable AI.” *ACM Computing Surveys* 55, no. 13s (December 31, 2023): 1–42. <https://doi.org/10.1145/3583558>.
- Nugraha, Muhammad Raihan. “Jenis Alat Bukti Sah Menurut KUHAP Baru.” *Hukumonline*, 2026. <https://www.hukumonline.com/klinik/a/jenis-alat-bukti-sah-menurut-kuhap-baru-lt657ae25924ac9/>.
- Pakpahan, Jun Triono, Elly Sudarti, and Erwin Erwin. “Pertanggungjawaban Pidana Perbuatan Ujaran Kebencian Yang Berkonten SARA Dalam Perspektif Peraturan Perundang-Undangan.” *Journal of Law, Education and Business* 2, no. 2 (September 30, 2024): 851–71. <https://doi.org/10.57235/jleb.v2i2.2540>.
- Pasquale, Frank. “The New Laws of Robotics.” Brooklyn Law School, 2021. <https://lawnotes.brooklaw.edu/issue/spring-2021/the-new-laws-of-robotics/>.
- Patsakis, Constantinos, David Arroyo, and Fran Casino. “The Malware as a Service Ecosystem,” 371–94, 2025. https://doi.org/10.1007/978-3-031-66245-4_16.
- Pavliukh, O.A., and H.F. Sanzharova. “Crime Attribution as a Critical Cybersecurity Issue.” *Juridical Scientific and Electronic Journal*, no. 9 (2024): 303–6. <https://doi.org/10.32782/2524-0374/2024-9/72>.
- Putra, I Made Walesa. “Asas Kesalahan Terkait Pertanggungjawaban Pidana Atas Tindak Pidana Dalam Pelaksanaan Jabatan Notaris.” *Acta Diurnal Jurnal Ilmu Hukum Kenotariatan* 8, no. 1 (2024): 116–31. <https://doi.org/10.23920/acta.v8i1.1958>.
- Radyananda, Basya, Faisal Abdaud, and Gamlan Dagani. “Analisis Limitasi Pertanggungjawaban Pidana Dalam Kejahatan Manipulasi Digital Di Indonesia.” *Nomos: Jurnal Penelitian Ilmu Hukum* 6, no. 1 (2026): 1–7. <https://doi.org/10.56393/nomos.v6i1.4273>.
- Räz, Tim. “Understanding Risk with FOTRES?” *AI and Ethics* 3, no. 4 (November 6, 2023): 1153–67. <https://doi.org/10.1007/s43681-022-00223-y>.
- Rizki, Mochamad Januar. “Mengenali Konsep Baru Jenis Pemidanaan Dalam KUHPP Nasional.” *Hukumonline*, 2024. <https://www.hukumonline.com/berita/a/mengenali-konsep-baru-jenis-pemidanaan-dalam-kuhp-nasional-lt662de997a2036/>.
- Saputra, Adji, Kristiawanto Kristiawanto, and Mohamad Ismed. “Rekonstruksi Penegakan Hukum Tindak Pidana Siber Di Indonesia.” *Seikat: Jurnal Ilmu Sosial, Politik Dan Hukum* 3, no. 1 (February 9, 2024): 63–70. <https://doi.org/10.55681/seikat.v3i1.1186>.
- Shumate, J Nicholas, Eden Rozenblit, Matthew Flathers, Carlos A Larrauri, Christine Hau, Winna Xia, E Nicholas Torous, and John Torous. “Governing AI in Mental Health: 50-State Legislative Review.” *JMIR Mental Health* 12 (October 31, 2025): e80739–e80739. <https://doi.org/10.2196/80739>.
- Slamet, Slamet. “Pendeteksi Botnet Malware DDOS Untuk Mencegah Serangan Distributed Denial of Service.” *SPIRIT: Journal of Computing and Cybernetic System* 16, no. 2

- (November 30, 2024). <https://doi.org/10.53567/spirit.v16i2.361>.
- Teller, Marina. "The Contribution of Law in the Regulation of Artificial Intelligence: Thinking about Algorithmic Democracy." *Journal of Artificial Intelligence for Sustainable Development* 1, no. 1 (January 1, 2024): 1–5. <https://doi.org/10.69828/4d4kmc>.
- Windani, Cynthia Ayu. "Strategi Dan Tantangan Predictive Policing Di Era Big Data Bagi Masyarakat Modern." *Deviance Jurnal Kriminologi* 7, no. 2 (December 31, 2023): 101–20. <https://doi.org/10.36080/djk.2385>.
- Wiraguna, Sidi Ahyar. "Metode Normatif Dan Empiris Dalam Penelitian Hukum: Studi Eksploratif Di Indonesia." *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum* 3, no. 3 (November 30, 2024): 57–65. <https://doi.org/10.59818/jps.v3i3.1390>.
- Zejneli, Rina, and Besa Arifi. "Criminal Responsibility (Insanity Defense)." *SEEU Review* 17, no. 2 (December 1, 2022): 120–38. <https://doi.org/10.2478/seeur-2022-0092>.
- Zoppolato, Davide Giacomo, and Paolo Davide Farah. "China's Path to Modernization and Legal Pluralism: Transplants and the Belt and Road Initiative." *Asian Journal of Law and Society* 12, no. 2 (June 17, 2025): 109–44. <https://doi.org/10.1017/als.2025.7>.