



Legal Politics of the Criminal Justice System in Dealing with Cybercrime in the Era of Digital Transformation to Realize Justice in Criminal Law Enforcement in Indonesia

^{1st} Umar Dinata, ²Ike Sumawaty

^{1,2} University of Muhammadiyah Riau

*email: umardinata@umri.ac.id, ikesumawaty@umri.ac.id

ABSTRACT

Keywords:

Legal Politics,
criminal justice
system,
cybercrime,
digital
transformation

Digital transformation has changed the patterns and characteristics of crime to become increasingly complex, organized, and cross-jurisdictional, posing new challenges for the criminal justice system in Indonesia. Adaptive legal politics is the main prerequisite to ensure that criminal law policies can accommodate technological developments while ensuring legal certainty, justice, and utility. This research aims to analyze the legal politics of the criminal justice system in dealing with cybercrime in the era of digital transformation and to reconstruct criminal law policies to realize justice in criminal law enforcement in Indonesia. The research uses a juridical-normative method with a legislative and conceptual approach. The research data is in the form of secondary data obtained through literature studies on laws and regulations, scientific literature, and previous research results, then analyzed qualitatively by descriptive-systematic analysis techniques. The results of the study show that the legal politics of the criminal justice system still face various obstacles in the form of regulatory disharmony, limitations in electronic evidence arrangements, weak coordination between law enforcement, and suboptimal protection for victims of cybercrime. Therefore, the reconstruction of criminal law policy needs to be directed at harmonizing regulations, strengthening restorative justice, protecting victims, digitizing the criminal justice system, increasing the capacity of law enforcement officials, and strengthening national and international cooperation. The reconstruction is expected to be able to realize a criminal justice system that is adaptive, fair, oriented towards the protection of human rights, and responsive to the development of digital technology.

1. INTRODUCTION

Digital transformation has fundamentally changed people's living systems, patterns of economic activities, government systems, and public service mechanisms in Indonesia. The development of information technology, cloud computing, artificial intelligence, big data, and the Internet of Things (IoT) has created cyberspace as a new arena of social interaction that is no longer limited by the country's territorial jurisdiction. Digitalization at this time can encourage increased national efficiency, innovation, and productivity, but at the same time it also gives birth to new forms of crime that have different characteristics from conventional crimes. Digital transformation has become a global phenomenon that changes the pattern of social, economic, and governance interactions. The wider use of information and communication technology has encouraged efficiency in various sectors of life. But on the other hand, the development of technology has also given rise to various new forms of crime known as cybercrime (Jumanudin 2026).

Cybercrime is developing very quickly through the use of digital technology, the anonymity of perpetrators, the use of cross-border networks, and the ability to eliminate electronic

traces, thus posing a serious challenge to Indonesia's criminal justice system. Unlike conventional crimes, which generally have locus delicti and relatively easy to identify perpetrators, cybercrime allows perpetrators to carry out attacks from various jurisdictions simultaneously using fake identities, *virtual private networks* (VPNs), encryption, *dark web* networks, and *cryptocurrency* technology which complicates the tracking process. The complexity of technology is one of the main factors that complicates the proof process. Rapid developments in information and communication technology have created new loopholes that can be exploited by cybercriminals. This condition causes law enforcement officials to face difficulties in the process of investigation, investigation, proof, and the implementation of court decisions because most of the evidence is in the form of electronic data which is easy to change, move, hide, and even delete in a matter of seconds (Nurul Aini 2024).

The complexity of cybercrime is increasing along with the development of technologies based on *Artificial Intelligence* (AI), *Internet of Things* (IoT), *cloud computing*, and blockchain technology that not only provide benefits to society, but are also used by criminals to increase the effectiveness of attacks. Phenomena such as digital identity theft, *online fraud*, *ransomware* attacks, *malware* spread, personal data theft, illegal trade through *the dark web*, and crypto-asset-based money laundering show that cybercrime has developed into transnational crimes that have economic, social, political, and national security impacts. In fact, various cyberattacks on the country's strategic infrastructure have the potential to disrupt the stability of public services and national resilience if not anticipated through an adaptive law enforcement system.

From the perspective of the criminal *justice system*, the characteristics of cybercrime raise various fundamental problems. Indonesia's criminal justice system is basically built based on the conventional crime paradigm that places the crime scene, physical evidence, and the existence of the perpetrator as the main elements in the evidentiary process. On the other hand, in cybercrime, most evidence is in the form of *electronic evidence* which requires digital *acquisition* methods, digital *forensic* analysis, and strict *chain of custody* mechanisms so that the integrity of evidence is maintained during the judicial process. Without these technical capabilities, the proof of cyber crimes has the potential to fail even though substantially a criminal act has occurred. Another problem that is no less important is the *cross-border nature* of cybercrime. Internet infrastructure allows servers, victims, perpetrators, service providers, and data storage locations to be in different jurisdictions. This situation raises problems regarding law enforcement authority, extradition of perpetrators, electronic data exchange, *mutual legal assistance*, and harmonization of international regulations. Therefore, the eradication of cybercrime cannot rely only on national legal instruments, but also requires effective international cooperation through mutual legal assistance mechanisms, the exchange of digital intelligence information, and the strengthening of international legal diplomacy. The variation in laws regarding cybercrime between countries also adds to the difficulties in dealing with these types of crimes because there is often no strong international agreement on how to deal with these crimes, creating a legal vacuum that is exploited by the perpetrators. Cybercrime can have far-reaching and damaging impacts on the global economy, national security, and international relations. For example, ransomware attacks can affect the operations of companies in different countries and disrupt international economic chains (Clara Ignatia Tobing, 2024).

From a legal political perspective, the dynamics of cybercrime show that law *lags behind technology*. Legal politics is the basic policy of the state in determining the direction of formation, renewal, and implementation of laws to achieve state goals. Therefore, the politics of criminal law must be able to produce regulations that are adaptive, responsive, and anticipatory to the development of digital technology without ignoring the principles of the rule of law, protection of human rights, legal certainty, justice, and utility. Criminal law reform is not only about the formation of legal norms, but also touches on institutional reform, increasing the capacity of law enforcement officials, strengthening electronic evidence, and integrating digital technology in the entire process of the criminal justice system (Alfendo Yefta Argastya, 2024).

In Indonesia, regulations regarding cybercrimes have undergone development through various legal instruments, including Law Number 11 of 2008 concerning Information and

Electronic Transactions as amended last by Law Number 1 of 2024, the National Criminal Code (Law Number 1 of 2023), the latest Procedural Law Number 20 of 2025, as well as various sectoral regulations regarding personal data protection and cybersecurity. However, the development of digital technology is taking place much faster than the formation of regulations. This condition causes a *regulatory lag*, which is a situation when the law lags behind the development of society so that various new modes of crime have not received adequate regulation. As a result, law enforcement officials often face difficulties in determining the legal basis, obtaining electronic evidence, confiscating digital data, and carrying out cross-jurisdictional cooperation against perpetrators outside Indonesian territory.¹ However, the dynamics of technological developments are taking place much faster than regulatory developments, so there are still various gaps in norms (*legal gaps*) and insynchronizations between regulations that have an impact on the effectiveness of law enforcement against cybercrime. This problem is even more evident when law enforcement officials have to deal with artificial intelligence-based crime models, *deepfakes*, *automated cyber attacks*, and transactions using digital assets that have not been fully accommodated in the national criminal law system.

Based on this description, it can be understood that cybercrime is not just a new development in the form of a criminal act, but has changed the paradigm of the criminal justice system as a whole. Its characteristics of being anonymous, cross-border, high-technology-based, and dependent on electronic evidence require the reconstruction of criminal law policies, strengthening electronic evidence regulations, increasing the capacity of law enforcement officials, and developing international cooperation so that Indonesia's criminal justice system is able to respond to the challenges of digital crime effectively, accountably, and fairly. Therefore, research on the Legal Politics of the Criminal Justice System in Dealing with Cybercrime in the Era of Digital Transformation to Realize Justice in Criminal Law Enforcement in Indonesia has academic and practical urgency as a foundation for legal reform that is responsive to the development of digital technology.

2. IMPLEMENTATION METHOD

This research is a juridical-normative legal study, which focuses on analyzing the provisions of applicable laws and regulations as positive laws in Indonesia. Secondary data for this study were collected through literature studies related to legal issues or problems raised. The secondary data is then analyzed qualitatively with a systematic approach to produce conclusions that are in accordance with the problem being studied. (Ali, Z. 2021) Research data is presented in clear, effective, orderly, logical, and concise sentences, making it easier to analyze and discuss research problems.

3. RESULTS AND DISCUSSION

1. Legal Politics of the Criminal Justice System in Dealing with Cybercrime in the Era of Digital Transformation

Digital transformation has changed the characteristics or forms of crime from conventional crime to *cyberspace-based* crimes that are anonymous, cross-jurisdictional, and make intensive use of information technology. These changes require a legal politics that is not only oriented towards the formation of criminal law norms, but also on the reform of the criminal justice system as a whole. The politics of criminal law in the context of cybercrime must be understood as a state policy to build a legal system that is adaptive to the development and advancement of digital technology and is able to provide

¹ Adinda Lola Sariani Dinda, "The Effectiveness of Law Enforcement Against Cybercrime in Indonesia," *AL-DALIL: Journal of Social, Political, and Legal Sciences*, Vol. 2, No. 2 (2024).

legal certainty and justice (Mohammad Alfian, 2025). Normatively, Indonesia already has a number of legal bases contained in the Electronic Information and Transaction Law, the Personal Data Protection Law, and the new Criminal Code. However, technological developments take place much faster than the legislative process, causing *regulatory lag*, which is a condition when the law lags behind the digital social reality. Recent research shows that Indonesia's cyber law politics are still dominated by a penal approach through law enforcement and criminal sanctions, while non-penal approaches such as digital literacy and strengthening a cybersecurity culture have not developed optimally. In law enforcement practice, the main problem lies in electronic proof. Digital evidence has the characteristic that it is easy to change, move, and even delete in seconds. As a result, investigators, public prosecutors, and judges are required to have adequate digital forensic competence. Research on the effectiveness of law enforcement against cyber crime shows that the biggest obstacles are not only in the substance of the law, but also in the limited human resources, the lack of digital literacy of law enforcement officials, and the complexity of technical proof in the digital realm (Ade Fatimah Zura, 2025).

In addition to the problem of proof, Indonesia's criminal justice system also faces structural challenges in the form of low integration between law enforcement agencies. The police, prosecutor's office, courts, correctional institutions, the State Cyber and Cryptography Agency, and related ministries are still working within a sectoral framework, even though the characteristics of cybercrime require cross-agency and cross-border coordination (Soetardi Tri Cahyono, 2025). Concretely, the political weaknesses of the criminal justice system can be seen from three aspects. First, the aspect of legal substance, namely the lack of harmonization of regulations regarding electronic evidence, digital data confiscation, cross-border jurisdiction, and digital corporate accountability. Second, the aspect of legal structure, namely the limitations of digital forensic laboratories, the lack of cyber investigators, and the uneven digital competence of judges and prosecutors. Third, the aspect of legal culture, namely low public awareness of cybersecurity and personal data protection (Medi Islamta Sembiring, 2026).

To overcome problems based on legal phenomena at the moment, the legal politics of the criminal justice system must be reconstructed through a more responsive approach to digital transformation. The first reconstruction is the harmonization of regulations between the ITE Law, the Personal Data Protection Law, the Criminal Code, and the Criminal Code Number 20 of 2025 so that there is no disharmony in norms in handling cyber cases. The transformation of political law in strengthening cyber law regulations shows that the renewal of the ITE Law and the new Criminal Code is a strategic step towards regulations that are more adaptive to technological developments and cyber threats (M Sihotang, 2025). The second reconstruction is the modernization of the criminal proof system. The state needs to establish national standards regarding the collection, storage, examination, and presentation of electronic evidence based on *the principle of chain of custody*. Strengthening digital forensic laboratories and certifying the competence of cyber investigators is an urgent need to ensure the integrity of digital evidence at trial. The third reconstruction is the strengthening of international cooperation. Since most cybercrime is transnational, national legal politics should support mechanisms for *mutual legal assistance*, *joint investigation*, and cross-border electronic data exchange. Without international cooperation, the process of tracking perpetrators and recovering digital assets will experience significant obstacles. The fourth reconstruction is the integration of penal and non-penal policies. Recent research shows that a combination of law enforcement, digital education, technical capacity building, and

collaborative cyber governance is more effective in reducing cybercrime rates than a repressive approach alone. Therefore, criminal law politics must develop an *integrated cyber governance* model that places law, technology, education, and community participation as a single national strategy.

An important finding from this discussion is that the political direction of the Indonesian criminal justice system is still in the transition phase from the conventional paradigm to the digital *justice paradigm*. This shift requires changes not only in laws and regulations, but also in institutional design, human resource capacity, and community legal culture. Thus, the effectiveness of the criminal justice system in dealing with cybercrime in the era of digital transformation is highly dependent on the state's ability to build an adaptive, integrated, and legal politics oriented towards the protection of citizens' digital rights (Jumanudin Juku and Zum Noversa Riala, 2026).

2. Reconstruction of criminal law policies to realize justice in Cybercrime Criminal Law Enforcement in the Digital Transformation Era in Indonesia

The reconstruction of criminal law policy is a strategic agenda in the reform of the national legal system to realize law enforcement that is not only oriented towards legal *certainty*, but also on substantive justice and legal benefits. So far, criminal law policy in Indonesia is still dominated by the retributive paradigm, which places prison as the main instrument for resolving cases. This approach has not been able to fully resolve legal conflicts comprehensively because it focuses more on punishing perpetrators than recovering victims, restoring social relations, and preventing the recurrence of criminal acts. Various studies have shown that this orientation contributes to the increase in overcrowding of correctional institutions, high recidivism, and low victim satisfaction with the criminal justice process (Hadiya Noor and Ranti Suminar Endah, 2025).

In the context of national criminal law reform, policy reconstruction must be directed at a paradigm shift from *offender-oriented justice* to *balanced justice* that places the interests of the state, victims, perpetrators, and society proportionately. The update is reflected in the development of criminal objectives in the national Criminal Code and criminal procedure law reform that begins to accommodate restorative justice mechanisms as part of criminal case resolution. However, recent research shows that these regulations still require clearer normative and procedural parameters so as not to cause disparities in implementation among law enforcement officials (Mirwansyah, and Irwan Jaya Diwirya, 2026). The reconstruction of criminal law policy must also touch on three main components of the legal system. First, the substance of the law, namely the harmonization between the Criminal Code, the Criminal Code, and various sectoral regulations so that there is no overlap in regulations regarding punishment, termination of prosecution based on restorative justice, victim protection, and criminal execution. Second, the legal structure, namely increasing the capacity of investigators, public prosecutors, judges, and correctional officers through continuous education, strengthening integrity, and the use of information technology in the judicial process. Third, legal culture, which is to build public awareness that the settlement of criminal cases is not always synonymous with imprisonment, but can be done through mechanisms that provide recovery for victims and real responsibility from the perpetrators. This approach will strengthen the legitimacy of the criminal justice system while increasing public trust in law enforcement (Sunnah, 2026).

In addition, the reconstruction of criminal law policy needs to strengthen the protection of victims as the main subject in the criminal justice system. So far, victims

have often been positioned only as a means of proof, while the rights to restitution, rehabilitation, and psychological recovery have not been optimally protected. Therefore, criminal law policies in the future must integrate effective restitution mechanisms, victim recovery services, supervision of the implementation of restorative agreements, and victim participation in every stage of the judicial process. This approach is in line with the development of modern criminal law which views the success of law enforcement not only from the severity of the crime imposed, but also from the level of recovery of victim losses and the creation of social reconciliation (M. Natsir Asnawi, 2026).

The reconstruction of criminal law policy in law enforcement against cybercrime in Indonesia must be directed at the formation of a criminal law system that is adaptive to the development of digital technology, oriented towards the protection of human rights, and able to realize a balance between legal certainty, justice, and utility. The development of *borderless* cybercrime, using *artificial intelligence*, *cryptocurrency*, *dark web*, and encryption technology has caused conventional criminal law instruments to no longer be able to answer the complexity of digital crime. This condition demands a change in the paradigm of law enforcement from a purely repressive approach to *an integrated digital criminal justice system* that combines technology-based preventive, repressive, restorative, and predictive approaches (oetardi Tri Cahyono, 2025). Concretely, this research produces five formulations of criminal law policy reconstruction.

First, harmonization is needed between the provisions in Law Number 1 of 2023 concerning the Criminal Code, the Information and Electronic Transactions Law and its amendments, the Personal Data Protection Law, and various other sectoral regulations so that an integrated cybercrime regulatory system is created and no longer causes overlapping norms. The harmonization provides legal certainty for the classification of cybercrimes, criminal liability, and a uniform electronic proof mechanism. (Wiarti, J. 2024)

Second, policy reconstruction is directed at strengthening *the digital forensic ecosystem* through increasing the capacity of investigators, prosecutors, judges, and digital forensic laboratories. The study found that the effectiveness of evidence in cybercrime cases is still influenced by limited human resources, digital investigative technology, and inter-agency coordination. Therefore, the development of a national digital forensic laboratory, improving the competence of law enforcement officials, and the use of artificial intelligence for the analysis of electronic evidence are urgent needs in the modern criminal justice system (Bayu Sujatmiko, 2026).

Third, this research produces a *Smart Criminal Justice System model*, which is a criminal law enforcement system that integrates digital technology at all stages of the criminal justice process ranging from electronic reporting, digital investigation, electronic evidence management, inter-agency data exchange, to integrated supervision of the implementation of criminal judgments. The model accelerates the law enforcement process, increases transparency, minimizes abuse of authority, and strengthens the accountability of law enforcement agencies in the era of digital transformation.

Fourth, the reconstruction of criminal law policy must integrate the principle of *restorative justice* in the settlement of certain cybercrime cases that cause individual losses and do not threaten national security. This approach places victims as the center of legal protection through the provision of restitution, psychological rehabilitation, digital data recovery, electronic reputation recovery, and supervision of the implementation of restorative agreements. Thus, the success of law enforcement is not only measured by the severity of the crime imposed on the perpetrators, but also by the level of success in

restoring victims' rights and the creation of sustainable cyberspace security (Fitri Arianti Saputri, 2024).

Fifth, this study recommends strengthening international cooperation in countering cybercrime through mutual *legal assistance* mechanisms, exchange of cyber intelligence information, standardization of digital evidence, and the development of a national cybercrime coordination center connected to international institutions. Given the characteristics of cybercrime that are cross-border, the effectiveness of law enforcement can no longer depend on national jurisdiction alone, but rather requires criminal law governance that is collaborative, responsive, and based on digital technology (Muhammad Rifaid, 2025). Thus, the concrete results of this study confirm that the reconstruction of criminal law policy in the era of digital transformation is not enough to be carried out through changes in the substance of laws and regulations, but must be followed by institutional transformation, digitalization of the criminal justice system, strengthening the capacity of law enforcement officials, protecting victims' rights, and developing integrated national cybersecurity governance. The reconstruction model is expected to be able to realize a modern, adaptive, fair, and consistent criminal law enforcement system based on the values of Pancasila and the development of global information technology. (Faisal, F., & Rustamaji, M. 2021).

1. CONCLUSION

The legal politics of the criminal justice system in dealing with cybercrime and the development of digital transformation require a comprehensive, adaptive, and justice-oriented reconstruction. Although Indonesia already has various legal instruments, such as the ITE Law, the Personal Data Protection Law, the Criminal Code, and the Criminal Code, rapid technological developments have caused *regulatory lags* that affect the effectiveness of law enforcement. Therefore, political and legal reform needs to be directed at the harmonization of material and formal criminal law, modernization of electronic evidence through the implementation of *the chain of custody*, strengthening the capacity and integrity of law enforcement officials, and increasing international cooperation in dealing with transnational cybercrime. Reconstruction must also shift the purely retributive criminal paradigm towards *balanced justice* by paying attention to the interests of the state, victims, perpetrators, and society proportionately. Victim protection needs to be strengthened through restitution, rehabilitation, and the consistent *and accountable implementation of restorative justice*. Thus, the criminal justice system not only functions to punish perpetrators, but also to prevent crime, recover victims, maintain people's digital rights, and build public trust. The reconstruction is ultimately expected to realize *digital justice* and reform of national criminal law that is effective, humane, responsive, and fair.

2. ADVICE

- a. Reconstruction of cybercrime regulations and proof systems the next research is suggested to examine in more depth the harmonization model of material and formal criminal law regulations in handling cybercrime, especially related to the position, validity, authentication, and *chain of custody* mechanism of electronic evidence.
- b. Development of a digital justice-based criminal justice system model *the next research* needs to be directed at the formulation of an integrated technology-based criminal justice system model, starting from the stages of investigation, investigation,

prosecution, examination in court, to the implementation of decisions. The model needs to integrate artificial intelligence and information technology in a measurable manner while ensuring transparency, accountability, personal data protection, human rights, and *due process of law principles*.

- c. Strengthening the *balanced justice* approach and protecting cybercrime victims The next research is suggested to develop a criminal model that balances the interests of the state, perpetrators, victims, and society through *a balanced justice approach*. The focus of the study can be directed to the optimization of restitution, victim rehabilitation, *restorative justice*, and the mechanism for recovering losses due to cybercrime.

BIBLIOGRAPHY

- Ade Fatimah Zura et al, "The Effectiveness of Law Enforcement against Hacking Cybercrime Based on the ITE Law in Indonesia", *AT-TAHDIS: Journal of Hadith Studies and Education* Vol 3 No 1 (2025)
- Adinda Lola Sariani Dinda, "The Effectiveness of Law Enforcement Against Cybercrime in Indonesia," *AL-DALIL: Journal of Social, Political, and Legal Sciences*, Vol. 2, No. 2 (2024).
- Agatha, C., & Rahaditya, R. Fragmented digital forensic standards in Indonesian criminal evidence. *Indonesian Journal of Law and Economics Review*, Vol 21, No 2. 2026.
- Alfendo Yefta Argastya, "Countermeasures to Cyber-Terrorism Crimes through the Politics of Criminal Law," *Jurist-Diction*, Vol. 7, No. 2, 2024.
- Anggraeniko, L. S., Ambarwati, A., & Utami, F. R. Admissibility of digital evidence in Indonesia: Criminal–civil implications for the chain of custody and evidentiary validity. *Priviet Social Sciences Journal*, vol 6, no 4. 2026.
- Bayu Sujatmiko, Ramlani Lina Sinaulan, and St. Laksanto Utomo, "The Transformation of Law Enforcement in the Criminal Code Number 1 of 2023 by the National Police," *ISO Journal: Journal of Social, Political and Humanities Sciences*, 2026.
- Clara Ignatia Tobing, *Sanaa Law Journal*, Volume 10, No 2, 2024
- Faisal, F., & Rustamaji, M. Reform of the criminal law pillar in the Criminal Code Bill. *Udayana Journal of Master of Law*, Vol 10, No 2, (2024)
- Fajriansyah, A., Siregar, R. A., & Panggabean, M. L. Criminal law reform in the digital era: An analysis of the new Criminal Code. *Journal of the Law of the Mimbar Justitia*, Vol 11, No1. 2025.
- Fitri Arianti Saputri, "Implications of the Implementation of Law Number 1 of 2023 Concerning the Criminal Code (New KUHP) on Restorative Justice Practices in Indonesia," *Jurispro Law Review*, Vol. 1, No. 2, 2024.
- Galfadillah, K. M., Zabril, A., & Nabila, G. Implementation of *Mutual Legal Assistance* (MLA) on electronic evidence that has been carried out by digital forensics in *cybercrime* between Indonesia and China. *RIGGS: Journal of Artificial Intelligence and Digital Business*, Vol 5, No 1, 2026.
- Galfadillah, K. M., Zabril, A., & Nabila, G. *Implementation of Mutual Legal Assistance* (MLA) on electronic evidence that has been carried out by digital forensics in *cyber crime* between Indonesia and China. *RIGGS*, Vol 5, No 1, 2026

- Hadiya Noor and Ranti Suminar Endah, "Reconstruction of Restorative Criminal Sanctions in Indonesia: *Reintegrative Shaming Perspective*," *Adil Ka'Talino: Journal of Law and Justice Discourse* 2025.
- Hardianto, A., Nawawi Arief, B., & Setiyono, J. The significance of computer forensics in electronic documents as evidence in criminal law. *Legal Horizon Journal*, Vol 14, No 2. 2023.
- Januri, Mirwansyah, and Irwan Jaya Diwirya, "Criminal Law Policy in the Application of Restorative Justice in the Renewal of the Indonesian Criminal Code," *Muara Hukum: Scientific Journal of Law and Public Administration* 2026
- Jumanudin Juku and Zum Noversa Riala, "Criminal Accountability of Cyber Crime Perpetrators in the Digital Era", *Indonesian Journal of Criminal Law* Vol 8 No 1 2026
- Jumanudin, *Indonesia Journal of Criminal Law*, Vol. 8, No. 1, June, 2026
- Laksono, A. S., & Patmawanti, B. The Politics of Criminal Law Reform with Pancasila Character. *Unes Journal of Sound Justice*, Vol 8, No 4, 2025
- M Sihotang, "Legal Political Transformation in Strengthening Cyber Law Regulation in Indonesia", *Syntax Admiration* Vol 6 No 1 2025
- M. Natsir Asnawi et al., "Restorative Justice from the Perspective of Progressive Legal Philosophy: Reconstructing the Paradigm of Criminal Law Enforcement in Indonesia," *Judge: Jurnal Hukum* (2026).
- Medi Islamta Sembiring et al., "Legal Protection for Victims of Cybercrime in the Indonesian Criminal Justice System", *Berajah Journal* Vol 6 No 4 2026
- Mohammad Alfian, "The Politics of Criminal Law in Countering Cybercrime in Indonesia: A Criminological Analysis on the Effectiveness of Penal and Non-Penal Policies", *Prosecutor: Journal of Legal and Political Studies* Vol 3 No 4 2025
- Muhammad Rifaid et al., "Transformation of Indonesian Criminal Justice Paradigm: Analysis of the Integration of Restorative Justice Principles in the National Criminal Code (Law No. 1 of 2023)," *Lex Journal: Law and Justice Studies*, Vol. 9, No. 3, 2025
- oetardi Tri Cahyono, Wina Erni, and Taufik Hidayat, "Reconstruction of Criminal Law against Cybercrime in the Indonesian Criminal Justice System," *Dame Journal of Law*, Vol. 1, No. 1, 2025
- Pase, A. T., & Fernando, Z. J. Dark Web Crime: Criminal Law Challenges in the Era of Cybercrime. *The Indonesian Journal of International Clinical Legal Education*, Vol 7, No 1. 2025
- Pratama, B. G. A., Pramono, A., & Ekaningsih, L. Digital justice: The challenges of proving and enforcing criminal law in the era of cyber anonymity. *Lex Journal: Law and Justice Studies*, Vol 10, No2, 2026.
- Purwaningsih, R., & Putranto, R. D. Juridical Review of the Determination of Locus Delicti in Cyber Crime in Relation to Criminal Law Reform Efforts in Indonesia. *Mimbar Keadilan*, Vol 16, No 1, 2023

-
- Putra, G. R. A. The position of digital evidence in the Indonesian criminal justice system: Reconceptualizing the regulation and strengthening *of the chain of custody* in the *era of cyber-enabled crime*. *THE NEWSLETTER*, Vol 8, No 7.2026
- Shidiq, M. P. Characteristics Cyber Crime and Dynamics of the Implementation Locus Delicti Theory by Law Enforcement Officials in Indonesia. *Adjudication: Journal of Legal Sciences*, Vol 8, No 2. 2024
- Soetardi Tri Cahyono, Wina Erni and Taufik Hidayat, "Reconstruction of Criminal Law against Cybercrime in The Indonesian Criminal Justice System", *Dame Journal of Law* Vol 1 No 1 2025
- Sunnah, "Reconstruction of Restorative Justice in the New Criminal Code: Philosophical Foundations, Normative Design, and Challenges of Victim Protection," *Mustika Justice* 2026
- Wiarti, J. Legality of electronic evidence in cyber crime cases. *Ahmad Dahlan Indonesian Law Journal*, Vol 1, No 2, (2024)
-



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/)
