Journal of Strafvordering:
https://nawalaeducation.com/index.php/JOSI/index
Jurnal Hukum Pidana Vol.2 No.6,January 2026
E-ISSN : 3046-8620
DOI : https://doi.org/10.62872/vt6zyw84

Countering Cybercrime in A Criminal Law Perspective: The Challenges of Law Enforcement in The Digital Age

Angga Aldilla Gussman[1]✉, Raudhotul Jannah[2],
Universitas Jambi, Indonesia[1], Sekolah Tinggi Ilmu Pertanian Berau, Indonesia[2]
e-mail: * anggagussman775@gmail.com [1]

Entered :November !3, 2025 Revised :December 23, 2025
Accepted : January 04, 2026 Published : January 28, 2026

ABSTRACT

The development of information technology has given birth to cybercrime as a form of modern criminality that challenges the foundations of conventional criminal law. Cybercrime is not only non-territorial and complex, but also has a broad impact on the public, economic, and security interests of the country. This research aims to analyze the normative construction of cybercrime in the Indonesian criminal law system, examine the harmonization of its regulation between Law Number 19 of 2016 concerning Electronic Information and Transactions and Law Number 1 of 2024 concerning the Criminal Code, and identify the challenges of criminal law enforcement in the digital era. The research method used is normative juridical with a legislative, conceptual, and systematic approach. The results of the study show that cybercrime regulation still faces the problem of unclear formulation of delicacies, fragmentation of norms, and potential disharmonization between sectoral laws and national criminal law codification. In addition, cyber criminal law enforcement is faced with electronic proof constraints, limited capacity of the apparatus, and the complexity of cross-border jurisdictions. This condition creates a gap between the normative goals of criminal law and law enforcement practices. Therefore, it is necessary to harmonize and integrate more comprehensive cybercrime regulations so that criminal law is able to provide legal certainty, justice, and human rights protection in a balanced manner in the digital era.

Keywords : Cybercrime; Criminal Law; Law Enforcement.

INTRODUCTION

The development of digital technology has driven a significant transformation in the pattern of social, economic, and administrative activities of the state, which at the same time has opened up space for the emergence of cybercrime as a form of modern crime. Cybercrime is no longer sporadic, but systemic and organized, taking advantage of technological gaps and regulatory weaknesses. The character of this crime shows a shift of locus delicti from physical space to cyberspace that is non-territorial. This condition challenges the principle of legality and the principle of territoriality which has been the foundation of criminal law. Criminal law is required to respond to this phenomenon adaptively without sacrificing the principle of legal certainty. Cybercrime

also causes significant economic losses, including in the taxation and state revenue sectors.[1] Therefore, countering cybercrime cannot be separated from the agenda of protecting the country's fiscal interests. The relationship between cybercrime and the tax system is becoming increasingly relevant as the economy digitizes. This meeting point demands the reading of criminal law in an integrated manner with national fiscal policy.

The transformation of the digital economy has direct implications for the national tax system, as responded to through Law Number 7 of 2021 concerning the Harmonization of Tax Regulations. The HPP Law marks the state's efforts to align fiscal instruments with the realities of the information technology-based economy. Transaction digitization opens up the potential for tax evasion, data manipulation, and electronic-system-based crime. This practice is not only an administrative violation, but has the potential to develop into a criminal act with a cyber dimension.[2] Cybercrime in the field of taxation shows a strong wedge between criminal law and tax law. The HPP Law implicitly requires the support of an effective criminal law regime to ensure compliance and enforcement.[3] Without an adaptive criminal mechanism, tax harmonization risks losing coercion. Criminal law enforcement is the ultimate instrument of remedium that remains relevant in maintaining the integrity of the tax system. Thus, the effectiveness of the HPP Law cannot be separated from the capacity of criminal law in dealing with cybercrime.

Indonesia's positive legal construction in responding to cybercrime is mainly based on Law Number 19 of 2016 as an amendment to the Electronic Information and Transaction Law. This law provides a normative basis for the criminalization of acts that abuse electronic systems. However, the regulation of cyber crime still faces conceptual and technical problems in its implementation. Some of the formulations of delicacies are broad and have the potential to cause differences in interpretation. This situation has an impact on the inconsistency of law enforcement and uncertainty for legal subjects. In the realm of digital taxation, the weakness of the formulation of cyber crimes can be used to disguise technology-based tax crimes. The HPP Law that emphasizes transparency and compliance requires the support of precise criminal norms. The insynchronization between the ITE Law and fiscal policy can weaken the goal of harmonization. Therefore, the integration of cyber criminal norms is an important prerequisite for the success of tax reform.

The change in the paradigm of national criminal law through Law Number 1 of 2024 as a new codification of the Criminal Code also affects the perspective on cybercrime. The new Criminal Code prioritizes a modern approach that is more responsive to the development of society and technology. Cybercrime is beginning to be placed as part of a crime that has a broad impact on the public and state interests. The principle of criminal responsibility in the new Criminal Code opens up space for the imposition of sanctions against corporations. This approach is relevant in the context of cybercrime in the economic and tax fields that often involve digital business entities. The

---

[1] Tawil, S., & Tarawneh, A. (2025). Technology and the law: countering cybercrime and fraud in the digital age. In *Artificial Intelligence in the Digital Era: Economic, Legislative and Media Perspectives* (pp. 1095-1105). Cham: Springer Nature Switzerland.

[2] Nosál, J. (2023). Crime in the digital age: A new frontier. In *The Implications of Emerging Technologies in the Euro-Atlantic Space: Views from the Younger Generation Leaders Network* (pp. 177-193). Cham: Springer International Publishing.

[3] Batrachenko, T., Lehan, I., Kuchmenko, V., Kovalchuk, V., & Mazurenko, O. (2024). Cybercrime in the context of the digital age: analysis of threats, legal challenges and strategies. *Multidisciplinary Science Journal*, *6*.

integration between the new Criminal Code and the ITE Law is an inevitable normative need. The HPP Law as a strategic fiscal policy requires the support of the criminal regime in line with the spirit of the new codification. Harmonization between laws is a challenge in a plural legal system. Without this synchronization, the effectiveness of countering cybercrime will be fragmented.

The law enforcement aspect of cybercrime presents serious challenges at the evidentiary stage. Electronic evidence has the character of being easily altered, copied, or deleted, thus demanding special technical expertise.[4] Law enforcement officials often face limited human resources and digital forensic infrastructure. This condition has an impact on the low success rate of disclosing cybercrime cases. In cases related to digital taxation, the difficulty of proving has the potential to hinder the optimization of state revenue. The HPP Law that relies on data and electronic systems requires a guarantee of the integrity of digital evidence. Weaknesses in criminal law enforcement will have direct implications for the effectiveness of fiscal policy. Countering cybercrime is not enough with written norms alone, it is necessary to strengthen institutional capacity so that criminal law can function in real terms.[5] Synergy between criminal policy and fiscal policy is key in answering this challenge.

The transnational dimension of cybercrime further complicates the enforcement of national criminal law. The perpetrator can operate from a different jurisdiction with the victim's location and electronic servers. This situation raises jurisdictional issues and cross-border law enforcement. International cooperation is an important element in combating cybercrime. In the context of taxation, the practice of profit shifting and concealment of digital assets often involves cross-border schemes. The HPP Law is designed to strengthen the national tax base in the midst of economic globalization. Without the support of criminal law enforcement that is able to penetrate state borders, this goal is difficult to achieve. National criminal law needs to be aligned with international instruments related to cybercrime. Lagging behind in international cooperation has the potential to be exploited by criminals, therefore, a global perspective is a necessity in formulating policies to combat cybercrime.[6]

The relationship between criminal law and tax administration law shows increasingly complex dynamics in the digital era. Tax administration violations can easily metamorphose into technology-based criminal acts. The line between administrative error and cybercrime is getting thinner. The HPP Law seeks to rearrange the balance between administrative and criminal sanctions. The placement of criminal sanctions as the ultimate remedium requires clear and measurable criteria. The lack of clarity in these criteria risks causing legal uncertainty. The new ITE Law and the Criminal Code need to be read systematically to support the policy. A partial approach to cybercrime will weaken the consistency of the legal system. The integration of criminal and fiscal norms is a rational demand in the modern legal state. The harmonization of the substance of the law is the foundation for fair law enforcement.

---

[4] Wahyudi, B. R. (2025). Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Teknologi AI. *INNOVATIVE: Journal Of Social Science Research*, *5*(1), 3436-3450.

[5] Wardana, A. P. (2024). Hukum Pidana dan Perlindungan Data Pribadi: Upaya Menanggulangi Kejahatan Siber di Era Digital di Indonesia. *Pustaka: Jurnal Ilmu Politik dan Hukum*, *1*(1), 20-25.

[6] Mokobombang, M., Darwis, Z., & Mokodenseho, S. (2023). Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam Penegakan Hukum Terhadap Kejahatan Digital. *Jurnal Hukum dan HAM Wara Sains*, *2*(6), 517-525.

These overall dynamics show that countering cybercrime is a multidimensional agenda that cannot be separated from criminal law reform and fiscal policy. Cybercrime not only threatens individuals, but also the economic and financial stability of countries. The HPP Law represents the state's interest in maintaining fiscal sovereignty in the digital era. The success of this goal is highly dependent on the effectiveness of criminal law as an enforcement instrument. Law Number 19 of 2016 and Law Number 1 of 2024 provide a normative framework that needs to be optimized synergistically. Without coherent integration, the legal system will face fragmentation and overlapping authority. The challenges of law enforcement in the digital age demand a comprehensive, future-oriented approach. Criminal law is no longer reactive enough, but must be proactive and preventive. Thus, countering cybercrime is an integral part of efforts to maintain justice, legal certainty, and the sustainability of national development.

METHOD

The development of digital technology has driven a significant transformation in the pattern of social, economic, and administrative activities of the state, which at the same time has opened up space for the emergence of cybercrime as a form of modern crime. Cybercrime is no longer sporadic, but systemic and organized, taking advantage of technological gaps and regulatory weaknesses. The character of this crime shows a shift of locus delicti from physical space to cyberspace that is non-territorial. This condition challenges the principle of legality and the principle of territoriality which has been the foundation of criminal law. Criminal law is required to respond to this phenomenon adaptively without sacrificing the principle of legal certainty. Cybercrime also causes significant economic losses, including in the taxation and state revenue sectors.[7] Therefore, countering cybercrime cannot be separated from the agenda of protecting the country's fiscal interests. The relationship between cybercrime and the tax system is becoming increasingly relevant as the economy digitizes. This meeting point demands the reading of criminal law in an integrated manner with national fiscal policy.

The transformation of the digital economy has direct implications for the national tax system, as responded to through Law Number 7 of 2021 concerning the Harmonization of Tax Regulations. The HPP Law marks the state's efforts to align fiscal instruments with the realities of the information technology-based economy. Transaction digitization opens up the potential for tax evasion, data manipulation, and electronic-system-based crime. This practice is not only an administrative violation, but has the potential to develop into a criminal act with a cyber dimension.[8] Cybercrime in the field of taxation shows a strong wedge between criminal law and tax law. The HPP Law implicitly requires the support of an effective criminal law regime to ensure compliance and enforcement.[9] Without an adaptive criminal mechanism, tax harmonization risks losing coercion. Criminal law enforcement is the ultimate instrument of remedium that remains relevant in maintaining the integrity of the tax system. Thus, the effectiveness of

[7] Tawil, S., & Tarawneh, A. (2025). Technology and the law: countering cybercrime and fraud in the digital age. In *Artificial Intelligence in the Digital Era: Economic, Legislative and Media Perspectives* (pp. 1095-1105). Cham: Springer Nature Switzerland.

[8] Nosál, J. (2023). Crime in the digital age: A new frontier. In *The Implications of Emerging Technologies in the Euro-Atlantic Space: Views from the Younger Generation Leaders Network* (pp. 177-193). Cham: Springer International Publishing.

[9] Batrachenko, T., Lehan, I., Kuchmenko, V., Kovalchuk, V., & Mazurenko, O. (2024). Cybercrime in the context of the digital age: analysis of threats, legal challenges and strategies. *Multidisciplinary Science Journal*, *6*.

the HPP Law cannot be separated from the capacity of criminal law in dealing with cybercrime.

Indonesia's positive legal construction in responding to cybercrime is mainly based on Law Number 19 of 2016 as an amendment to the Electronic Information and Transaction Law. This law provides a normative basis for the criminalization of acts that abuse electronic systems. However, the regulation of cyber crime still faces conceptual and technical problems in its implementation. Some of the formulations of delicacies are broad and have the potential to cause differences in interpretation. This situation has an impact on the inconsistency of law enforcement and uncertainty for legal subjects. In the realm of digital taxation, the weakness of the formulation of cyber crimes can be used to disguise technology-based tax crimes. The HPP Law that emphasizes transparency and compliance requires the support of precise criminal norms. The insynchronization between the ITE Law and fiscal policy can weaken the goal of harmonization. Therefore, the integration of cyber criminal norms is an important prerequisite for the success of tax reform.

The change in the paradigm of national criminal law through Law Number 1 of 2024 as a new codification of the Criminal Code also affects the perspective on cybercrime. The new Criminal Code prioritizes a modern approach that is more responsive to the development of society and technology. Cybercrime is beginning to be placed as part of a crime that has a broad impact on the public and state interests. The principle of criminal responsibility in the new Criminal Code opens up space for the imposition of sanctions against corporations. This approach is relevant in the context of cybercrime in the economic and tax fields that often involve digital business entities. The integration between the new Criminal Code and the ITE Law is an inevitable normative need. The HPP Law as a strategic fiscal policy requires the support of the criminal regime in line with the spirit of the new codification. Harmonization between laws is a challenge in a plural legal system. Without this synchronization, the effectiveness of countering cybercrime will be fragmented.

The law enforcement aspect of cybercrime presents serious challenges at the evidentiary stage. Electronic evidence has the character of being easily altered, copied, or deleted, thus demanding special technical expertise.[10] Law enforcement officials often face limited human resources and digital forensic infrastructure. This condition has an impact on the low success rate of disclosing cybercrime cases. In cases related to digital taxation, the difficulty of proving has the potential to hinder the optimization of state revenue. The HPP Law that relies on data and electronic systems requires a guarantee of the integrity of digital evidence. Weaknesses in criminal law enforcement will have direct implications for the effectiveness of fiscal policy. Countering cybercrime is not enough with written norms alone, it is necessary to strengthen institutional capacity so that criminal law can function in real terms.[11] Synergy between criminal policy and fiscal policy is key in answering this challenge.

The transnational dimension of cybercrime further complicates the enforcement of national criminal law. The perpetrator can operate from a different jurisdiction with the victim's location and electronic servers. This situation raises jurisdictional issues and cross-border law enforcement. International cooperation is an important element in

[10] Wahyudi, B. R. (2025). Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Teknologi AI. *INNOVATIVE: Journal Of Social Science Research*, *5*(1), 3436-3450.

[11] Wardana, A. P. (2024). Hukum Pidana dan Perlindungan Data Pribadi: Upaya Menanggulangi Kejahatan Siber di Era Digital di Indonesia. *Pustaka: Jurnal Ilmu Politik dan Hukum*, *1*(1), 20-25.

combating cybercrime. In the context of taxation, the practice of profit shifting and concealment of digital assets often involves cross-border schemes. The HPP Law is designed to strengthen the national tax base in the midst of economic globalization. Without the support of criminal law enforcement that is able to penetrate state borders, this goal is difficult to achieve. National criminal law needs to be aligned with international instruments related to cybercrime. Lagging behind in international cooperation has the potential to be exploited by criminals, therefore, a global perspective is a necessity in formulating policies to combat cybercrime.[12]

The relationship between criminal law and tax administration law shows increasingly complex dynamics in the digital era. Tax administration violations can easily metamorphose into technology-based criminal acts. The line between administrative error and cybercrime is getting thinner. The HPP Law seeks to rearrange the balance between administrative and criminal sanctions. The placement of criminal sanctions as the ultimate remedium requires clear and measurable criteria. The lack of clarity in these criteria risks causing legal uncertainty. The new ITE Law and the Criminal Code need to be read systematically to support the policy. A partial approach to cybercrime will weaken the consistency of the legal system. The integration of criminal and fiscal norms is a rational demand in the modern legal state. The harmonization of the substance of the law is the foundation for fair law enforcement.

These overall dynamics show that countering cybercrime is a multidimensional agenda that cannot be separated from criminal law reform and fiscal policy. Cybercrime not only threatens individuals, but also the economic and financial stability of countries. The HPP Law represents the state's interest in maintaining fiscal sovereignty in the digital era. The success of this goal is highly dependent on the effectiveness of criminal law as an enforcement instrument. Law Number 19 of 2016 and Law Number 1 of 2024 provide a normative framework that needs to be optimized synergistically. Without coherent integration, the legal system will face fragmentation and overlapping authority. The challenges of law enforcement in the digital age demand a comprehensive, future-oriented approach. Criminal law is no longer reactive enough, but must be proactive and preventive. Thus, countering cybercrime is an integral part of efforts to maintain justice, legal certainty, and the sustainability of national development.

PEMBAHASAN

1. Normative Construction of Cybercrime in the Indonesian Criminal Law System

Cybercrime represents a fundamental shift in the conception of criminal acts that have been assumed to be based on physical acts and certain geographical spaces. The development of information technology blurs the boundaries between private and public spaces, so that legal interests protected by criminal law have expanded. The national criminal law is no longer enough to be oriented only to the protection of public order in a conventional way. Cybercrime places data security, electronic system integrity, and digital trust as new legal interests. This change requires the reconstruction of criminal norms in order to be able to capture virtual social reality. Failure to respond to such changes has the potential to create a void of legal protection. The normative vacuum

[12] Mokobombang, M., Darwis, Z., & Mokodenseho, S. (2023). Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam Penegakan Hukum Terhadap Kejahatan Digital. *Jurnal Hukum dan HAM Wara Sains*, *2*(6), 517-525.

opens up space for impunity for technology-based criminals. Therefore, cybercrime must be understood as a structural challenge to national criminal law.[13]

Law Number 19 of 2016 seeks to answer these challenges through the criminalization of certain acts related to electronic systems. However, the formulation of the law shows a tendency to use technical terms that are not always accompanied by strict normative limits. The unclarity of the elements of the crime poses the risk of expanding interpretation by law enforcement officials, this risk has a direct impact on the principle of legal certainty guaranteed by the principle of legality.[14] Furious criminal norms have the potential to be used repressively against certain legal subjects. This situation creates tensions between the goals of law enforcement and the protection of human rights.[15] Criminal law loses legitimacy when used without strict normative parameters. Therefore, the construction of cybercrime crimes requires a critical evaluation of its formulation techniques. The evaluation is important to ensure that criminalization is carried out proportionately.

Another weakness in the normative construction of cybercrime lies in the approach to errors that is still classically oriented.[16] The concept of mens rea in traditional criminal law is difficult to apply to crimes involving automated systems and complex networks. Many cybercrimes occur through a series of digital processes that are not completely controlled directly by the perpetrators. This condition raises the problem of proving evil intentions and intentions. Reliance on the concept of pure intentionality has the potential to undermine the effectiveness of law enforcement. Criminal law is required to develop a more functional and realistic approach to error. Without conceptual reform, criminal law risks not being able to reach sophisticated cybercriminals. These risks indicate a gap between norms and practices. This gap needs to be overcome through the reformulation of criminal norms.

Law Number 1 of 2024 as a new codification of the national criminal law offers a more systematic reform framework. The new Criminal Code shifts the orientation of criminal law from a purely repressive approach to a balanced approach. The principle of criminal liability was extended to include corporations as subjects of law. This expansion is relevant because cybercrime is often committed through organizational structures or business entities. However, the integration of the new Criminal Code norms with sectoral regulation of cybercrime is not yet fully clear. This ambiguity has the potential to create a dualism of the arrangement. Dualism of norms can weaken the consistency of the criminal law system. Inconsistent criminal laws risk losing their binding power Therefore, the position of cybercrime must be affirmed within the framework of national codification.[17]

---

[13] Naro, W., Syatar, A., Amiruddin, M. M., Haq, I., Abubakar, A., & Risal, C. (2020). Shariah assessment toward the prosecution of cybercrime in indonesia. *International Journal*, *9*, 573.

[14] Saliro, S. S., Aminah, S., Jamaludin, J., Aprilsesa, T. D., & Kusryat, D. (2025). Virtual Police in the Indonesian Constitutional System: A Restorative Justice Approach to Cybercrime Prevention (An Empirical Study in Sambas Regency). *Jurnal Mahkamah: Kajian Ilmu Hukum Dan Hukum Islam*, *10*(1), 27-38.

[15] Muhammad, R., Sitompul, S. M., Zafarovich, T. S., & Embong, R. (2025). The Reduction of Criminal Justice Policy in Indonesia: Justice versus Virality. *Journal of Human Rights, Culture and Legal System*, *5*(2), 442-472.

[16] Anwary, I. (2022). The Role of Public Administration in combating cybercrime: An Analysis of the Legal Framework in Indonesia. *International Journal of Cyber Criminology*, *16*(2), 216-227.

[17] Suseno, S., Ramli, A. M., Mayana, R. F., Safiranita, T., & Aurellia Nathania Tiarma, B. (2025). Cybercrime in the new criminal code in Indonesia. *Cogent Social Sciences*, *11*(1), 2439543.

The position of Law Number 19 of 2016 as a sectoral law raises systematic problems in criminal law. The existence of criminal norms outside the Criminal Code often creates regulatory fragmentation. This fragmentation makes it difficult to establish a consistent criminal law doctrine. The new Criminal Code is intended to be the main reference in the interpretation of criminal law. However, cybercrime regulation is still outside the codification structure. This disintegration poses the risk of conflict of norms in judicial practice. Judges have the potential to face difficulties in determining which norms must be prioritized. This uncertainty has an impact on the quality of court decisions. Therefore, the normative construction of cybercrime needs to be placed explicitly in the national criminal law system. This placement is a prerequisite for legal certainty.[18]

Overall, the normative construction of cybercrime still shows a transitional character and is not yet fully mature. Attempts at criminalization have been made, but they have not been followed by conceptual and systematic consistency. Law Number 19 of 2016 and Law Number 1 of 2024 provide an important legal basis, but still leave room for criticism.[19] Criminal law should not stop at formal recognition of cybercrime. Normative reform based on critical and rational analysis is needed. Without these updates, criminal law has the potential to lag behind technological developments. Lag in the law will weaken the function of protecting the community. Therefore, the normative reconstruction of cybercrime is an urgent agenda for Indonesia's criminal law.

2. Harmonization of Cybercrime Regulation between the ITE Law and the National Criminal Code

Legal harmonization is a fundamental requirement for the effective functioning of the criminal law system. The existence of various criminal laws outside the Criminal Code requires normative alignment. The regulation of cybercrime shows the complexity of the relationship between general norms and specific norms. Law Number 19 of 2016 is designed as a special instrument to regulate information technology-based acts. Law Number 1 of 2024 functions as a general criminal law that is codifying. The relationship between the two cannot be allowed to run in parallel without normative coordination. Disharmony will create legal uncertainty and have the potential to harm legal subjects and weaken law enforcement.[20]

The application of the principle of lex specialis is often used as a justification to prioritize the ITE Law over the Criminal Code. However, the use of this principle mechanically risks ignoring the purpose of the codification of criminal law.[21] The new Criminal Code is intended as a systemic framework that unites all criminal norms. Specific norms should be placed in a coherent relationship with general norms. Without

[18] Mursyid, M., Putera, A., & Jannah, M. (2025). Rekonstruksi Peran Digital Forensik Dalam Penyidikan Tindak Pidana Siber: Analisis Kritis Terhadap Konstruksi Hukum Pidana di Indonesia. *Jurnal Tana Mana*, *6*(2), 289-296.

[19] Singgi, I. G. A. S. K., Suryawan, I. G. B., & Sugiartha, I. N. G. (2020). Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime). *Jurnal Konstruksi Hukum*, *1*(2), 334-339.

[20] Idris, M., Nurlani, M., & Aprita, S. (2024). PENGATURAN DAN PENEGAKAN HUKUM KEJAHATAN DUNIA MAYA (CYEBER CRIME): HARMONISASI REVISI UNDANG-UNDANG ITE DAN KUHP. *Lex LATA*, *6*(3).

[21] Irawati, A. C. (2023, December). Harmonization of'Cyber Crime'Articles in The National Criminal Code. In *The Virtual International Conference on Economics, Law and Humanities* (Vol. 2, No. 1, pp. 20-27).

coherence, the principle of lex specialis is a source of fragmentation. Fragmentation of norms makes it difficult to establish consistent law enforcement patterns. Consistency is an important element in the principle of equality before the law. Inconsistency in law enforcement will damage public trust, therefore, harmonization must go beyond the mere application of normative principles. Harmonization must be realized in accordance with the substance and purpose of the law.[22]

The difference in the sanction system between the ITE Law and the new Criminal Code shows the urgency of harmonization. Law Number 19 of 2016 still prioritizes prison sentences as the main instrument. This approach reflects a criminal paradigm that is retributive. The new Criminal Code introduces a variety of sanctions that are more oriented towards the purpose of the crime. This difference has the potential to create disparities in criminal sentencing. Disparities in punishment can lead to substantive injustice. This injustice will damage the legitimacy of the criminal law. Harmonization of sanctions is needed to ensure proportionality and rationality of punishment because without proportionality, the criminal offense loses its corrective and preventive functions.[23] Therefore, the alignment of the sanctions system is a basic need.

Corporate criminal liability is another aspect that demands serious harmonization. Cybercrime is often carried out through corporate structures or digital platforms. Law Number 19 of 2016 has recognized corporations as the subject of criminal law, but the regulation is limited. The new Criminal Code provides a more systematic framework for corporate accountability. The insynchronization of the two arrangements creates ambiguity in the application of the law. Corporations can take advantage of normative loopholes to avoid criminal liability. This condition weakens the reach of criminal law against large-scale cybercrime perpetrators. Harmonization is needed to strengthen corporate accountability. Without accountability, criminal law fails to protect the public interest. Therefore, the integration of corporate arrangements is a strategic agenda.

Harmonization also concerns the harmony of the penal objectives adopted by each law. The ITE Law tends to emphasize the protection of electronic systems and the deterrent effect. The new Criminal Code prioritizes a balance between retaliation, prevention, and rehabilitation. These differences in orientation have the potential to cause insynchronization in criminal practice. Inconsistent sentencing practices will result in inconsistent verdicts. This inconsistency has an impact on the community's sense of justice. The purpose of the punishment must be formulated coherently in order to be applied effectively. Philosophical harmonization is a prerequisite for normative harmonization. Without philosophical alignment, the harmonization of norms will be pseudo. Therefore, the alignment of the goals of the punishment must receive serious attention.

Overall, the harmonization of cybercrime regulation cannot be seen as a purely technical issue. Harmonization is an ideological and systemic process in the development of national criminal law. Law Number 19 of 2016 and Law Number 1 of 2024 must be read as a single legal system. A separate sectoral approach will undermine the effectiveness of law enforcement. Failed harmonization has the potential to create uncertainty and injustice. Criminal law requires a coherent structure to function

[22] Iu, K. Y., & Wong, V. M. Y. (2024). The trans-national cybercrime court: towards a new harmonisation of cyber law regime in ASEAN. *International Cybersecurity Law Review*, *5*(1), 121-141.

[23] Gustryan, M., & Sulaiman, A. (2025). The Urgency of Regulatory Reformulation and Strengthening the Capacity of Law Enforcers in Combating Cybercrime Through a Criminal Law Approach in Indonesia. *Greenation International Journal of Law and Social Sciences*, *3*(2), 221-229.

optimally. Without coherence, criminal law loses its regulatory power. Therefore, the harmonization of cybercrime must be placed as a priority for criminal law reform. This priority is important to answer the challenges of the digital era in a sustainable manner.

3. Challenges of Criminal Law Enforcement against Cybercrime in the Digital Era

Criminal law enforcement against cybercrime faces much more complex challenges than conventional crimes. The invisible nature of cybercrime makes it difficult to detect early. Law enforcement officials often rely on late victim reports. This delay has an impact on the loss of an important digital footprint. Without adequate traces, the investigation process becomes ineffective. These technical limitations show the structural unpreparedness of law enforcement officials. Normatively strong criminal law is not automatically effective in practice. The effectiveness of law enforcement requires adequate technical capacity support. Therefore, the challenges of law enforcement are structural and systemic.

The evidentiary aspect is a crucial point in cybercrime. Electronic evidence has a character that is easy to manipulate and replicate. The validity and integrity of evidence are often debated at trial. Law Number 19 of 2016 has recognized electronic evidence, but has not regulated technical standards in detail. The absence of this standard opens up space for differences in judges' judgments. Differences in judgment have the potential to cause inconsistency in the decision. This inconsistency undermines legal certainty. The new Criminal Code has not fully answered the technical problem of digital proof. Therefore, the challenge of proof remains the main obstacle to the enforcement of criminal law siber.[24]

The issue of jurisdiction is also a significant challenge in the enforcement of cybercrime laws. Cybercrime often involves perpetrators who are outside the country's territory. National criminal law is still based on classical territorial principles. This principle has limitations when dealing with cross-border crimes. The process of extradition and international cooperation often takes a long time. These delays reduce the effectiveness of law enforcement, without effective international cooperation, cybercriminals are difficult to reach.[25] Law Number 19 of 2016 has not regulated the cross-border mechanism comprehensively. The new Criminal Code also faces similar limitations. Therefore, law enforcement requires a transnational approach.

The institutional capacity of law enforcement officials is a determining factor for the success of cyber criminal law enforcement. The limitation of human resources who have digital expertise is the main obstacle. Digital forensic infrastructure is not yet equally available. This inequality creates disparities in the handling of cases. This disparity has the potential to cause procedural injustice. Uneven law enforcement undermines the principle of equality before the law. Public trust in criminal law depends on the professionalism of the authorities. The new Criminal Code requires officials who are able to translate norms progressively. Without institutional support, these demands are difficult to realize. Therefore, strengthening institutional capacity is an urgent need.

---

[24] Nicodemus, A. A. (2023). *Tantangan dalam Penegakan Hukum Pidana terhadap Kejahatan Siber di Era Digital* (Doctoral dissertation, Sekolah Tinggi Ilmu Hukum IBLAM).

[25] Ambawta, M., & Chaudhary, A. (2025). DIGITAL PLATFORMS AND THE CHANGING LANDSCAPE OF CRIME: CHALLENGES AND OPPORTUNITIES FOR LAW ENFORCEMENT. *Lex Localis: Journal of Local Self-Government*, *23*(10).

Cyber criminal law enforcement also faces a dilemma between the effectiveness of enforcement and the protection of human rights. Cybercrime often intersects with freedom of expression and privacy. Aggressive law enforcement has the potential to violate citizens' constitutional rights. Law Number 19 of 2016 is often criticized because it has the potential to be used in a repressive manner. The new Criminal Code seeks to balance the interests of law enforcement and the protection of rights. This balance is not easy to achieve in practice. Law enforcement officials need clear and strict guidelines. Without these guidelines, law enforcement risks exceeding the limits of authority. Therefore, the protection of human rights must be an integral part of law enforcement.

Overall, the challenges of criminal law enforcement against cybercrime are multidimensional and interrelated. Normative, technical, and institutional challenges cannot be partially solved. Law Number 19 of 2016 and Law Number 1 of 2024 provide an important legal basis, but they are not fully adequate. The effectiveness of law enforcement depends on the synergy between norms and practices. Without synergy, criminal law will only be a symbolic instrument. The challenges of the digital era demand adaptive and reflective criminal law. The adaptation must be accompanied by continuous critical evaluation. Thus, cyber criminal law enforcement can respond to the demands of justice and legal certainty in a balanced manner.

CONCLUSION

Based on the overall discussion, cybercrime is a modern criminal phenomenon that challenges the classical construction of national criminal law. The development of information technology has expanded the legal interests that must be protected, beyond the territorial and physical boundaries that have been the basis for the formulation of criminal acts. Law Number 19 of 2016 has provided a normative basis for the criminalization of cybercrime, but it still shows weaknesses in the clarity of the formulation of the delicacy and conceptual consistency. These weaknesses have implications for potential legal uncertainty and the risk of excessive application of norms. Criminal law reform through Law Number 1 of 2024 offers a more systematic and responsive codification framework to social and technological dynamics. However, the existence of sectoral regulation of cybercrime outside the new Criminal Code poses a serious normative harmonization challenge. The insynchronization between general norms and specific norms has the potential to weaken the consistency of criminal law enforcement. In addition to normative issues, law enforcement against cybercrime also faces technical and institutional obstacles, especially in electronic evidence and the capacity of law enforcement officials. The challenges of cross-border jurisdiction further complicate the effectiveness of cyber criminal law enforcement. The situation shows that there is a gap between the normative goals of criminal law and the reality of law enforcement practices. Therefore, countering cybercrime requires an integrated, adaptive, and oriented approach to criminal law and human rights protection. With strong integration and harmonization, criminal law is expected to be able to respond to the challenges of cybercrime in the digital era in a sustainable manner.

REFERENCES

Ambawta, M., & Chaudhary, A. (2025). Digital Platforms And The Changing Landscape Of Crime: Challenges And Opportunities For Law Enforcement. Lex Localis: Journal of Local Self-Government, 23(10)..

Anwary, I. (2022). The Role of Public Administration in combating cybercrime: An Analysis of the Legal Framework in Indonesia. International Journal of Cyber Criminology, 16(2), 216-227.

Batrachenko, T., Lehan, I., Kuchmenko, V., Kovalchuk, V., & Mazurenko, O. (2024). Cybercrime in the context of the digital age: analysis of threats, legal challenges and strategies. Multidisciplinary Science Journal, 6.

Gustryan, M., & Sulaiman, A. (2025). The Urgency of Regulatory Reformulation and Strengthening the Capacity of Law Enforcers in Combating Cybercrime Through a Criminal Law Approach in Indonesia. Greenation International Journal of Law and Social Sciences, 3(2), 221-229.

Idris, M., Nurlani, M., & Aprita, S. (2024). Pengaturan Dan Penegakan Hukum Kejahatan Dunia Maya (Cyeber Crime): Harmonisasi Revisi Undang-Undang ITE dan KUHP. Lex LATA, 6(3).

Irawati, A. C. (2023, December). Harmonization of'Cyber Crime'Articles in The National Criminal Code. In The Virtual International Conference on Economics, Law and Humanities (Vol. 2, No. 1, pp. 20-27).

Iu, K. Y., & Wong, V. M. Y. (2024). The trans-national cybercrime court: towards a new harmonisation of cyber law regime in ASEAN. International Cybersecurity Law Review, 5(1), 121-141.

Mahlil Adriaman et al., Pengantar Metode Penelitian Ilmu Hukum (Padang: Yayasan Tri Edukasi Ilmiah, 2024).

Mokobombang, M., Darwis, Z., & Mokodenseho, S. (2023). Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam Penegakan Hukum Terhadap Kejahatan Digital. Jurnal Hukum dan HAM Wara Sains, 2(6), 517-525.

Muhammad, R., Sitompul, S. M., Zafarovich, T. S., & Embong, R. (2025). The Reduction of Criminal Justice Policy in Indonesia: Justice versus Virality. Journal of Human Rights, Culture and Legal System, 5(2), 442-472.

Mursyid, M., Putera, A., & Jannah, M. (2025). Rekonstruksi Peran Digital Forensik Dalam Penyidikan Tindak Pidana Siber: Analisis Kritis Terhadap Konstruksi Hukum Pidana di Indonesia. Jurnal Tana Mana, 6(2), 289-296.

Naro, W., Syatar, A., Amiruddin, M. M., Haq, I., Abubakar, A., & Risal, C. (2020). Shariah assessment toward the prosecution of cybercrime in indonesia. International Journal, 9, 573.

Nicodemus, A. A. (2023). Tantangan dalam Penegakan Hukum Pidana terhadap Kejahatan Siber di Era Digital (Doctoral dissertation, Sekolah Tinggi Ilmu Hukum IBLAM).

Nosál, J. (2023). Crime in the digital age: A new frontier. In The Implications of Emerging Technologies in the Euro-Atlantic Space: Views from the Younger Generation Leaders Network (pp. 177-193). Cham: Springer International Publishing.

Novea Elysa Wardhani, Sepriano, and Reni Sinta Yani, Metodologi Penelitian Bidang Hukum (Jambi: PT. Sonpedia Publishing Indonesia., 2025).

Peter Mahmud Marzuki, Penelitian Hukum (Jakarta: Kencana Prenada Media Group, 2011).

Rangga Suganda, "Metode Pendekatan Yuridis Dalam Memahami Sistem Penyelesaian Sengketa Ekonomi Syariah," Jurnal Ilmiah Ekonomi Islam 8, no. 3 (2022): 2859, https://doi.org/10.29040/jiei.v8i3.6485.

Saliro, S. S., Aminah, S., Jamaludin, J., Aprilsesa, T. D., & Kusryat, D. (2025). Virtual Police in the Indonesian Constitutional System: A Restorative Justice Approach to Cybercrime Prevention (An Empirical Study in Sambas Regency). Jurnal Mahkamah: Kajian Ilmu Hukum Dan Hukum Islam, 10(1), 27-38.

Singgi, I. G. A. S. K., Suryawan, I. G. B., & Sugiartha, I. N. G. (2020). Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime). Jurnal Konstruksi Hukum, 1(2), 334-339.

Suseno, S., Ramli, A. M., Mayana, R. F., Safiranita, T., & Aurellia Nathania Tiarma, B. (2025). Cybercrime in the new criminal code in Indonesia. Cogent Social Sciences, 11(1), 2439543.

Tawil, S., & Tarawneh, A. (2025). Technology and the law: countering cybercrime and fraud in the digital age. In Artificial Intelligence in the Digital Era: Economic, Legislative and Media Perspectives (pp. 1095-1105). Cham: Springer Nature Switzerland.

Wahyudi, B. R. (2025). Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Teknologi AI. INNOVATIVE: Journal Of Social Science Research, 5(1), 3436-3450.

Wardana, A. P. (2024). Hukum Pidana dan Perlindungan Data Pribadi: Upaya Menanggulangi Kejahatan Siber di Era Digital di Indonesia. Pustaka: Jurnal Ilmu Politik dan Hukum, 1(1), 20-25..