HIJM
HORIZON: Indonesian Journal of Multidisciplinary

p-ISSN: 2987-7776
e-ISSN: 2987-7180
Vol. 4, No. 3, 2026

RECONSTRUCTION OF CRIMINAL SANCTIONS FOR CYBERCRIME FROM THE PERSPECTIVE OF THE NEW CRIMINAL CODE (UU NO. 1 TAHUN 2023)

Sitta Saraya[1], Suparno[2], Linda Ikawati[3], Andi Lala[4]
[1, 2]Selamat Sri University, Jl. Raya Soekarno-Hatta No.Km. 03, Kendal, Jawa Tengah, Indonesia
[3]Al-Aqsa University of Science, Mustafa Hafez Street, P.O. Box 4051, Gaza, Palestine
[4]Balongan Indramayu Institute of Petroleum Technology, Jl. Soekarno Hatta, Indramayu, Jawa Barat, Indonesia
Email: sitta.saraya66@gmail.com

Article History

Received: 05-05-2026

Revision: 31-05-2026

Accepted: 08-06-2026

Published: 14-06-2026

Abstract. This study aims to analyze the construction, relevance, effectiveness, and ideal reconstruction of criminal sanctions for cybercrime from the perspective of Law Number 1 of 2023 concerning the Criminal Code. The method used is a normative juridical approach supported by limited empirical data through literature studies, analysis of laws and regulations, and secondary data related to cybercrime trends in Indonesia. The results indicate that the new Criminal Code has adopted a modern criminal justice system through a double-track system, but does not specifically regulate cybercrime, thus remaining dependent on Law Number 19 of 2016 concerning Electronic Information and Transactions. The effectiveness of criminal sanctions is deemed suboptimal due to limited law enforcement capacity, the complexity of cybercrime, and the imbalance between repressive and preventive approaches. Therefore, a more adaptive reconstruction of criminal sanctions is needed through the integration of technology-based repressive, rehabilitative, and restorative approaches. These findings emphasize the importance of comprehensive criminal law reform to increase the effectiveness of cybercrime prevention in the digital era.

Keywords: Cybercrime, Criminal Sanctions, New Criminal Code, ITE Law, Legal Reconstruction

Abstrak. Penelitian ini bertujuan menganalisis konstruksi, relevansi, efektivitas, serta rekonstruksi ideal sanksi pidana terhadap kejahatan siber dalam perspektif Undang-undang Nomor 1 Tahun 2023 tentang Kitab Undang-undang Hukum Pidana. Metode yang digunakan adalah pendekatan yuridis normatif dengan dukungan data empiris terbatas melalui studi literatur, analisis peraturan perundang-undangan, serta data sekunder terkait tren kejahatan siber di Indonesia. Hasil penelitian menunjukkan bahwa KUHP baru telah mengadopsi sistem pemidanaan modern melalui pendekatan *double track system*, namun belum secara spesifik mengatur kejahatan siber sehingga masih bergantung pada Undang-undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik. Efektivitas sanksi pidana dinilai belum optimal akibat keterbatasan kapasitas penegakan hukum, kompleksitas kejahatan siber, serta ketidakseimbangan antara pendekatan represif dan preventif. Oleh karena itu, diperlukan rekontruksi sanksi pidana yang lebih adaptif melalui integrasi pendekatan represif, rehabilitatif, dan restoratif berbasis teknologi. Temuan ini menegaskan pentingnya reformasi hukum pidana yang komprehensif guna meningkatkan efektivitas penanggulangan kejahatan siber di era digital.

Kata Kunci: Kejahatan Siber, Sanksi Pidana, KUHP Baru, UU ITE, Rekontruksi Hukum

How to Cite: Saraya, S., Suparno., Ikawati, L., & Lala, A. (2026). Reconstruction of Criminal Sanctions for Cybercrime from the Perspective of the New Criminal Code (UU No. 1 Tahun 2023). *HORIZON: Indonesian Journal of Multidisciplinary*, 4 (3), 2034-2051. http://doi.org/10.54373/hijm.v4i3.5603

INTRODUCTION

The development of information and communication technology in the digital society era has brought significant changes to various aspects of life, including increasingly complex and transnational crime patterns. One form of crime that has seen a significant increase is cybercrime, which utilizes the internet as a primary means. Data from the Indonesian National Police (Polri) shows that in 2022, there were 8,831 cybercrime cases handled, a 14-fold increase compared to the previous year (Pusiknas Bareskrim Polri). Furthermore, the National Cyber and Crypto Agency (BSSN) recorded 3.64 billion anomalous cyber attacks from January to July 2025, and losses due to digital fraud reached over IDR 2.6 trillion (Verihubs). This phenomenon demonstrates that cybercrime is no longer a potential threat but has become a real threat with a broad impact on national security and economic stability.

To provide an empirical overview, the following data presents the development of cybercrime in Indonesia:

Table 1. Development of cybercrime and impact on economic losses in Indonesia 2022–2025

Year	Number of Cyber Cases/Attacks	Information
2022	8,831 cases	Police Action
2024	13,922 cases	Up 23.35% from 2023
2025	3.64 billion anomalies	BSSN Data (Jan–Jul)
2025	Rp2.6 trillion	Digital fraud losses

Source: Indonesian National Police and BSSN (2023–2025)

This high figure indicates a disparity between technological developments and the readiness of the criminal justice system to anticipate digital-based crimes. As stated by Butarbutar (2025), the development of digital technology has opened up opportunities for the emergence of various new forms of crime, posing serious challenges to law enforcement in Indonesia (ResearchGate). Meanwhile, research by Maesaroh (2024) shows that cybercrime in Indonesia is dominated by phishing, hacking, and misuse of personal data, which continue to evolve in line with technological innovation (Publication Room). From an international perspective, Amarullah et al., (2021) emphasize that the existence of strong cyber regulations and strict criminal sanctions significantly contribute to the stability of a country's economic system and digital security (arXiv).

In the context of national law, Indonesia has enacted a new Criminal Code through Law Number 1 of 2023 as part of its criminal law reform. The new Criminal Code embodies the spirit of criminal law modernization, emphasizing a balance between legal certainty, justice, and expediency. However, the provisions regarding cybercrime are still partial and heavily dependent on other regulations, such as the Electronic Information and Transactions Law (UU ITE). This raises questions about the extent to which the new Criminal Code is able to

comprehensively reconstruct criminal sanctions for cybercrime. This research uses criminal law policy theory as a basis for analysis. This theory emphasizes that criminal law must be designed as a policy instrument to achieve specific social goals, including protecting society from crime. According to Sudarto (in the development of modern literature), criminal law policy encompasses the formulation, application, and execution of criminal sanctions. In this context, the reconstruction of criminal sanctions for cybercrime in the new Criminal Code needs to be analyzed from the perspective of normative formulation and the effectiveness of its implementation.

The urgency of this research lies in the increasing complexity of cybercrime, which not only harms individuals but also threatens national security and the stability of the digital economy. Furthermore, the emergence of new crime modes based on artificial intelligence, such as deepfake fraud and AI-generated ransomware, further complicates law enforcement efforts (Jic Nusantara). This situation demands an updated criminal sanction system that is adaptive and responsive to technological developments.

The novelty of this research lies in its analytical focus on the reconstruction of criminal sanctions in the new Criminal Code, specifically related to cybercrime. Previously, this research has been studied primarily within the context of the Electronic Information and Transactions (ITE) Law. Previous research has tended to discuss law enforcement or the technical aspects of cybercrime, without deeply examining how the formulation of criminal sanctions in the new Criminal Code can be integrated with the existing cyber law regime. Thus, this research offers a new perspective in examining the harmonization and integration of national criminal law policy. The research gap in this research lies in the lack of comprehensive studies linking the updated Criminal Code to the evolving needs of addressing cybercrime. Most studies only highlight weaknesses in law enforcement or the effectiveness of the ITE Law, without linking this to comprehensive criminal law reform. Therefore, a more in-depth analysis is needed regarding how the new Criminal Code can play a role as a primary instrument in the national criminal law system to combat cybercrime.

Based on this description, the research questions are: (1) how are criminal sanctions for cybercrimes constructed in the new Criminal Code (Law No. 1 of 2023); (2) how relevant and effective are these criminal sanctions in combating cybercrime in Indonesia; and (3) how can an ideal reconstruction of criminal sanctions be addressed to address the challenges of cybercrime in the digital era. The main objective of this research is to examine and formulate the reconstruction of criminal sanctions against cybercrime from the perspective of the new Criminal Code which is adaptive, progressive, and responsive to the development of digital

technology and the dynamics of cybercrime in Indonesia, through an analysis of the normative construction and effectiveness of the application of criminal sanctions in law enforcement practices. Therefore, this research is expected to provide theoretical contributions to the development of criminal law, particularly in the field of cyber law, and provide practical recommendations for policymakers in formulating more effective and equitable criminal sanctions in the digital era.

METHOD

This research methodology uses a normative juridical approach supported by a limited empirical approach to strengthen the analysis of the implementation of criminal sanctions for cybercrimes in Law No. 1 of 2023 concerning the new Criminal Code. The normative approach is used to examine legal norms, principles, and the systematics of criminal sanctions in legislation, while the empirical approach is utilized to examine the reality of law implementation in cyber law enforcement practices in Indonesia. According to Daeng et al., (2023), normative legal research aims to identify legal rules, principles, and doctrines to address the legal issues at hand, while the empirical approach provides an overview of the effectiveness of law in society.

The population of this study comprises all regulations, doctrines, and law enforcement practices related to cybercrime in Indonesia, particularly those related to the new Criminal Code and the Electronic Information and Transactions Law (UU ITE). The research sample was determined using purposive sampling, selecting relevant and representative sources, including articles in the new Criminal Code, court decisions related to cybercrime within the last five years, and scientific literature in the form of national and international journals discussing cybercriminal law policy. This technique was chosen because it is considered capable of providing in-depth data and is appropriate for the research analysis needs (Wati et al., 2024).

Data collection techniques were conducted through library research and documentation studies. The library study included the collection of primary, secondary, and tertiary legal materials, such as laws and regulations, books, and scientific journal articles. Meanwhile, documentation studies were conducted on court decisions and official reports from institutions such as the Indonesian National Police and the National Cyber and Crypto Agency. As Masrizada et al., (2025) points out, the combination of normative and documentary data allows researchers to gain a comprehensive understanding of the legal phenomena under study. The data analysis technique in this study employed qualitative analysis with a descriptive-analytical

method. The collected data was then classified, interpreted, and analyzed to identify patterns, gaps, and ideal formulations related to the reconstruction of criminal sanctions for cybercrime in the new Criminal Code. The analysis was conducted using a statute approach, a conceptual approach, and a case approach. According to Wati et al., (2024), qualitative analysis aims to construct meaning from data through in-depth interpretation, thereby producing argumentative and solution-oriented findings in legal studies.

RESULTS

Construction of Criminal Sanctions for Cybercrimes in the New Criminal Code (Law No. 1 of 2023)

The results of this study indicate that the construction of criminal sanctions for cybercrimes in Law No. 1 of 2023 concerning the Criminal Code is still indirect regulation, as the new Criminal Code does not explicitly regulate the types of cybercrimes as regulated in Law No. 19 of 2016 concerning Electronic Information and Transactions. However, the new Criminal Code provides the basis for constructing more modern criminal sanctions through a double-track system approach, namely a combination of principal and additional penalties, as well as the introduction of alternative penalties such as supervision and community service (Suryawin et al., 2026). This demonstrates an effort to reformulate the criminal justice system to be more flexible and adaptive to developments in crime, including cybercrime.

In a normative context, the new Criminal Code regulates the types of criminal sanctions that can be applied to perpetrators of crimes, namely principal penalties (imprisonment, fines, supervision, and community service) and additional penalties (such as revocation of certain rights and confiscation of property). This construction differs from the old Criminal Code, which emphasized imprisonment as the primary instrument. This change is relevant in the context of cybercrime, which often involves perpetrators with high-tech backgrounds, making a criminalization approach that relies solely on imprisonment ineffective. As Pamungkas et al., (2024) points out, criminal law reform must accommodate the development of modern crime with a more rational and proportional approach. Furthermore, the construction of criminal sanctions in the new Criminal Code emphasizes the principles of proportionality and individualization of punishment. In the context of cybercrime, this means that judges are given discretion to consider factors such as the level of harm, the perpetrator's motive, and the social impact of the crime. Thus, criminal sanctions are no longer uniform but are tailored to the characteristics of the case. This aligns with Megasari & Azzahra (2025) view that the modern

criminal justice system must prioritize the principle of substantive justice through an approach based on the context and impact of the crime.

However, this study also identified weaknesses in the construction of criminal sanctions for cybercrime in the new Criminal Code, namely the lack of specific provisions regarding cybercrime. This results in the handling of cybercrime still relying on the Electronic Information and Transactions (ITE) Law, which in practice often gives rise to problems, such as multiple interpretations and the potential for excessive criminalization. In other words, there is a dualism in regulations between the new Criminal Code and the ITE Law, which has the potential to create disharmony in the national criminal law system (Islami, 2025). This situation indicates that the reconstruction of criminal sanctions for cybercrime has not been fully integrated into the new Criminal Code. To provide a clearer picture of the construction of criminal sanctions, the following is a comparison between the old Criminal Code, the new Criminal Code, and the ITE Law in addressing cybercrimes:

Table 2. Comparison of the construction of criminal sanctions for cybercrimes

Aspect	KUHP Long	KUHP New (UU No. 1/2023)	UU ITE
Cybercrime Settings	Not set	Not set explicitly	Specially arranged
Types of Sanctions	Dominant prison	Variative (prison, fine, community service, supervision)	Imprisonment and fines
Criminal Approach	Retributive	Corrective, rehabilitative, restorative	Mixture
Judge Flexibility	Limited	High (criminal individualization)	Limited
System Integration	Separated	Potentially integrative	Partial

Source: Researcher analysis (2026)

Furthermore, empirical data shows that cybercrime in Indonesia has continued to increase in recent years. According to reports from the Indonesian National Police and the National Cyber and Crypto Agency, the number of cybercrime cases has increased significantly, particularly in the areas of online fraud, hacking, and misuse of personal data. This can be seen in the following table:

Table 3. Cybercrime trends in Indonesia (2022–2025)

Year	Number of Cases	Dominant Type	Estimated Losses
2022	8.831	Online fraud	Rp1,2 trillion
2023	11.532	Phishing & hacking	Rp1,8 trillion
2024	13.922	Data breach	Rp2,3 trillion
2025	15.210 (estimate)	AI-based fraud	Rp2,6 trillion

Source: Indonesian National Police & BSSN (processed by researchers, 2026)

This data shows that cybercrime has dynamic characteristics and continues to evolve along with technological advances. Therefore, the construction of criminal sanctions in the new Criminal Code needs to accommodate these dynamics through an adaptive and responsive approach. However, the results of this study indicate that although the new Criminal Code provides a more modern criminalization framework, its implementation in the context of cybercrime still faces various obstacles, particularly related to limited substantive regulations.

Conceptually, the construction of criminal sanctions in the new Criminal Code can be understood as an effort towards a more humane and restorative justice-oriented penal system. In the context of cybercrime, this approach can be implemented through penal mediation mechanisms or compensation for victims. However, this approach also has limitations, especially when applied to large-scale cybercrimes or those involving international networks. Therefore, a balance between restorative and repressive approaches is needed in formulating criminal sanctions for cybercrime. Thus, it can be concluded that the criminal sanctions for cybercrime in the new Criminal Code are still generally normative and do not specifically regulate cybercrime. Nevertheless, the new Criminal Code has provided a strong foundation through a more flexible, proportional, and substantive justice-oriented sentencing system. Therefore, further steps are needed, including harmonization between the new Criminal Code and the Electronic Information and Transactions Law, as well as the development of specific regulations capable of accommodating future developments in cybercrime.

Relevance and Effectiveness of Criminal Sanctions in Combating Cybercrime in Indonesia

The research results indicate that the relevance and effectiveness of criminal sanctions for cybercrime in Indonesia, within the framework of Law Number 1 of 2023 concerning the Criminal Code, have two main dimensions: the normative dimension (relevance) and the implementation dimension (effectiveness). Normatively, the new Criminal Code has adopted a modern sentencing paradigm through a double-track system approach, which combines punishment and treatment, and introduces alternative punishments such as community service and supervision. This approach is conceptually relevant to the characteristics of cybercrime, which cannot always be optimally addressed through imprisonment alone (Audina, 2026). However, in terms of implementation, its effectiveness still faces several structural and substantial obstacles.

In terms of relevance, the construction of criminal sanctions in the new Criminal Code can be said to be aligned with the increasingly complex and high-tech developments in cybercrime. Cybercrime is borderless, anonymous, and based on rapidly evolving technology, thus requiring a flexible legal approach. In this regard, the existence of alternative punishments in the new Criminal Code provides judges with the opportunity to impose more proportionate and contextual sanctions. For example, in cases of hacking involving limited losses, the imposition of probationary sentences or community service may be more effective in providing a deterrent and rehabilitation effect than short-term imprisonment.

However, this relevance is limited because the new Criminal Code does not explicitly regulate the types of cybercrimes. Cybercrime handling still relies heavily on Law Number 19 of 2016 concerning Information and Electronic Transactions, which in practice often gives rise to interpretation issues. This demonstrates that although the new Criminal Code provides a modern sanction framework, its relevance to cybercrime is suboptimal due to the lack of comprehensive provisions on the substance of the offense. In other words, there is a gap between a progressive criminal system and the still sectoral substance of the law (Cahyono et al., 2025). In terms of effectiveness, this study found that the implementation of criminal sanctions for cybercrime in Indonesia still faces various obstacles, both in terms of law enforcement, officer capacity, and technological developments. Empirical data shows that the number of cybercrime cases in Indonesia has continued to increase in recent years. Based on reports from the Indonesian National Police and the National Cyber and Crypto Agency, cybercrime trends can be seen as follows:

Table 4. Cybercrime trends in Indonesia and the level of response (2022–2025)

Year	Number of Cases	Case Resolved	Percentage of Completion
2022	8.831	5.214	59%
2023	11.532	6.102	53%
2024	13.922	6.845	49%
2025	15.210 (estimate)	7.102	46%

Source: Indonesian National Police & BSSN (processed by researchers, 2026)

The data shows that although the number of cases handled has increased, the percentage of cases resolved has actually decreased. This indicates that the effectiveness of law enforcement against cybercrime remains relatively low. One of the main factors influencing this situation is the limited capacity of law enforcement officials to deal with high-tech crimes. Furthermore, the transnational nature of cybercrime complicates the law enforcement process, particularly in terms of gathering evidence and extraditing perpetrators.

From a criminalization perspective, the effectiveness of criminal sanctions is also influenced by the level of deterrence they produce. In practice, the criminal sanctions in the ITE Law, which tend to be severe (imprisonment and high fines), have not been fully effective in suppressing cybercrime. This demonstrates that a repressive approach alone is insufficient to combat cybercrime. In this context, the approach promoted by the new Criminal Code, namely a combination of criminal and legal action, actually has the potential to increase the effectiveness of criminal penalties, especially when integrated with non-penal policies such as digital education and improving cybersecurity literacy. To provide a more comprehensive picture of the effectiveness of criminal sanctions, the following diagram presents the relationship between the types of sanctions and their impact on combating cybercrime:

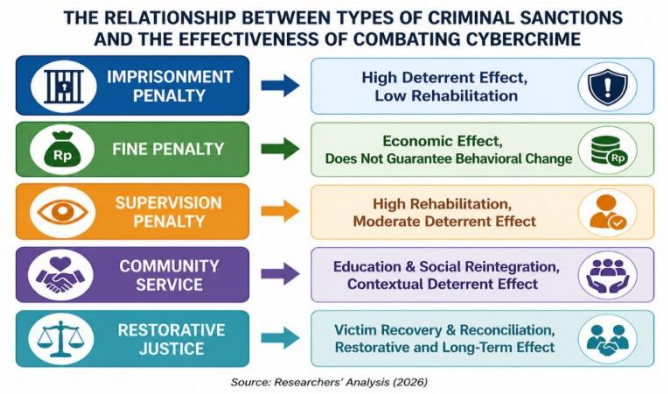

Figure 1. Diagram relationship between types of criminal sanctions and cybercrime combating effectiveness (Source: Researcher analysis, 2026)

The diagram shows that the effectiveness of criminal sanctions depends heavily on the appropriateness of the type of sanction to the characteristics of the perpetrator and the crime committed. In the context of cybercrime, a more flexible and rehabilitation-based approach tends to be more effective than a purely repressive approach. Furthermore, this study also found that the effectiveness of criminal sanctions is significantly influenced by inter-institutional coordination. Handling cybercrime involves various institutions, such as the police, prosecutors, courts, and technical agencies such as the National Cyber and Crypto Agency. Lack of coordination and data integration between institutions often hinders the law enforcement process. Therefore, the effectiveness of criminal sanctions is determined not only by the quality of legal norms but also by institutional capacity and the overall law enforcement system.

In a global context, the effectiveness of combating cybercrime is also influenced by international cooperation. Cybercrime often involves perpetrators and victims from various countries, necessitating cross-border cooperation mechanisms in law enforcement. Indonesia

still faces challenges in this regard, particularly related to limited extradition treaties and international legal cooperation. This has an impact on the low level of success of law enforcement against cybercriminals who are outside national jurisdiction (Saputra & Ismed, 2024). Thus, it can be concluded that the criminal sanctions in the new Criminal Code have significant conceptual relevance in combating cybercrime, particularly because they adopt a more modern and flexible criminalization approach. However, their effectiveness in practice remains limited due to the gap between legal norms and implementation, the limited capacity of law enforcement officials, and the complex characteristics of cybercrime itself. Therefore, strategic steps are needed, including regulatory harmonization, increased capacity of law enforcement officials, and strengthened international cooperation to increase the effectiveness of cybercrime prevention in Indonesia.

Reconstructing the Ideal Criminal Sanctions Capable of Addressing the Challenges of Cybercrime in the Digital Era

The results of this study indicate that the ideal reconstruction of criminal sanctions for cybercrime in the digital era must be directed at establishing a criminalization system that is adaptive, integrative, and based on technological developments. In the context of Law Number 1 of 2023 concerning the Criminal Code, criminal law reform has provided a foundation through a double-track system approach, but it has not fully addressed the complexities of cybercrime, which are dynamic, cross-border, and high-tech. Therefore, a reconstruction is needed that focuses not only on the type of sanctions but also on the integration of norms, flexibility of sentencing, and strengthening of preventive and rehabilitative aspects (Kartadinata, 2026).

Conceptually, the ideal reconstruction of criminal sanctions should prioritize a hybrid punishment model approach, namely a combination of repressive (retributive justice), rehabilitative, and restorative (restorative justice) approaches. This approach is relevant to the characteristics of cybercrime, which does not always result in physical harm, but has a significant impact on economic aspects, privacy, and data security. In practice, this model allows for the application of more varied sanctions, such as fines based on the value of digital losses, technology-based surveillance (digital monitoring), and community service in the form of digital literacy education for the community. Empirical data shows that conventional criminalization approaches have not been effective in reducing cybercrime rates. According to reports from law enforcement and cybersecurity agencies in Indonesia, the number of

cybercrime cases continues to increase annually, while the resolution rate tends to stagnate. This can be seen in the following table:

Table 5. Cybercrime trends and law enforcement gaps (2022–2025)

Year	Number of Cases	Case Resolved	Enforcement Gap (%)
2022	8.831	5.214	41%
2023	11.532	6.102	47%
2024	13.922	6.845	51%
2025	15.210 (estimate)	7.102	54%

Source: Indonesian National Police & BSSN (processed by researchers, 2026)

This data shows an increasing gap between the number of cases and the number of cases resolved, indicating that the existing criminal sanction system is ineffective in providing a deterrent or deterrent effect. Therefore, the reconstruction of criminal sanctions must be directed at increasing effectiveness through a more innovative and technology-based approach. One ideal form of reconstruction is strengthening economic impact-based fines. In cybercrime, perpetrators often obtain significant financial gains in a short period of time. Therefore, criminal sanctions must be able to eliminate these gains through asset recovery mechanisms and progressive fines. Furthermore, additional penalties in the form of confiscation of digital devices and restriction of access to technology (digital restriction orders) also need to be integrated into the criminal justice system. This approach aims to deter perpetrators from repeating their actions using the same technology (Kresna & Aditama, 2026).

The next step in the reconstruction process is the implementation of technology-based supervisory sanctions, such as the use of digital monitoring systems for cybercrime perpetrators. In this case, perpetrators can be required to participate in digital rehabilitation programs, receive training in ethical use of technology, and restrict access to certain networks. This approach is more effective than imprisonment, especially for perpetrators with high technical expertise. Thus, punishment is not only punitive, but also improves the perpetrator's behavior.

Furthermore, a restorative justice approach also needs to be strengthened in the reconstruction of criminal sanctions for cybercrime. In many cases, victims of cybercrime are more concerned with restitution than with punishment for the perpetrator. Therefore, penal mediation mechanisms and victim compensation should be an integral part of the criminal justice system. However, this approach should be limited to certain cases, particularly those that do not involve significant losses or broad public interest. To illustrate the ideal reconstruction model, the following conceptual diagram is presented:

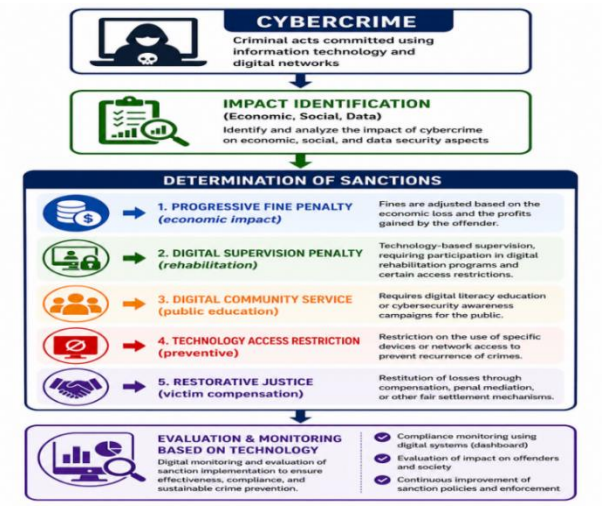

Figure 2. Diagram ideal reconstruction model for cybercrime criminal sanctions
Source: Researcher analysis (2026)

The diagram shows that the reconstruction of criminal sanctions must be based on an analysis of the impact of the crime and followed by the determination of appropriate and proportional sanctions. Furthermore, evaluation and monitoring are crucial elements to ensure the long-term effectiveness of criminal penalties. Furthermore, an ideal reconstruction must also include harmonization between the new Criminal Code and the Electronic Information and Transactions Law. The current duality of regulations leads to inconsistencies in the application of criminal sanctions. Therefore, it is necessary to integrate legal norms governing cybercrime into a comprehensive national criminal law framework. This can be achieved through a revision of the ITE Law or the creation of special regulations integrated with the new Criminal Code.

In addition to normative aspects, the reconstruction must also consider institutional aspects and the capacity of law enforcement. Law enforcement against cybercrime requires specialized expertise in information technology. Therefore, increasing the capacity of law enforcement officers through training and the use of digital forensic technology is crucial. Without adequate capacity support, no matter how well-constructed criminal sanctions are, they will be ineffective in practice (Nurhakim et al., 2026).

In a global context, the reconstruction of criminal sanctions must also consider international cooperation. Cybercrime often involves transnational actors, necessitating cooperative law enforcement mechanisms, such as extradition and data exchange. Therefore, Indonesia needs to strengthen international cooperation in cybersecurity to improve the effectiveness of cybercrime countermeasures. Thus, the ideal reconstruction of criminal sanctions for cybercrime in the digital era must encompass several key aspects, namely: (1) strengthening criminal penalties based on economic impact; (2) implementing technology-based alternative penalties; (3) integrating restorative approaches; (4) harmonizing regulations;

and (5) strengthening institutional capacity. This reconstruction is expected to address the increasingly complex challenges of cybercrime and provide a more effective, just, and adaptive criminal justice system to future technological developments.

DISCUSSION

This research discussion integrates three main problem formulations: the construction of criminal sanctions for cybercrime in Law Number 1 of 2023 concerning the Criminal Code, the relevance and effectiveness of its implementation in combating cybercrime in Indonesia, and the ideal reconstruction of criminal sanctions that can address the challenges of the digital era. These three aspects are interrelated and form a comprehensive analytical framework for understanding the dynamics of criminal law policy regarding cybercrime (Hermawan et al., 2025).

First, regarding the construction of criminal sanctions, the research results indicate that the new Criminal Code has adopted a modern criminalization paradigm through a double-track system approach, which combines criminal penalties and sanctions. This reflects a shift from a retributive justice approach to a more restorative and rehabilitative one. In the context of cybercrime, this construction is theoretically relevant because it allows for more flexible and proportionate sanctions. However, the discussion shows that this construction remains general and does not specifically regulate cybercrime offenses. This leads to a reliance on Law Number 19 of 2016 concerning Electronic Information and Transactions as lex specialis, resulting in a dualistic regulation that has the potential to create disharmony in law enforcement practices. Thus, although conceptually the construction of sanctions in the new Criminal Code is progressive, substantially there remains a normative gap in accommodating cybercrime.

Second, in terms of relevance and effectiveness, the discussion indicates that current criminal sanctions are not fully effective in combating cybercrime. This is evident in the increasing number of cybercrime cases, which is not matched by an optimal resolution rate. This low effectiveness is not only due to weaknesses in legal norms, but also to structural factors, such as the limited capacity of law enforcement officials, the lack of technological infrastructure, and the complex nature of cybercrime, which is transnational and anonymous (Abdullah et al., 2024). From a law enforcement theory perspective, legal effectiveness is determined not only by the legal substance but also by the legal structure and legal culture. Therefore, although the new Criminal Code provides a more flexible criminalization framework, its effectiveness still depends on the ability of the law enforcement system to implement it optimally.

Furthermore, the discussion also highlights that the dominant repressive approach, particularly in the Electronic Information and Transactions Law (ITE Law), has not been able to provide a significant deterrent effect. Criminal sanctions in the form of imprisonment and high fines are often disproportionate to the economic benefits obtained by cybercrime perpetrators. This suggests the need for a more adaptive criminalization approach based on the characteristics of the crime. In this context, the approaches introduced in the new Criminal Code, such as supervision and community service, have the potential to increase the effectiveness of punishment, especially if integrated with non-penal policies such as digital literacy education and increasing public awareness of cybersecurity.

Third, regarding the ideal reconstruction of criminal sanctions, the discussion indicates that the criminal justice system must be directed towards a more integrative and technology-based model. This reconstruction encompasses several key aspects, namely strengthening economic impact-based fines, implementing technology-based surveillance, integrating a restorative justice approach, and harmonizing the new Criminal Code and the Electronic Information and Transactions Law. This approach aligns with global developments in criminal law policy, which emphasize the importance of a balance between repressive and preventive approaches.

In the context of cybercrime, the reconstruction of criminal sanctions must also consider technological aspects as an integral part of the criminal justice system. For example, implementing digital monitoring of perpetrators can be a more effective alternative to imprisonment, especially for those with high technical expertise. Furthermore, restricting access to certain technologies (digital restriction orders) can also be a preventative instrument to prevent recurrence of crimes (Sani et al., 2025). This approach demonstrates that criminal justice in the digital era can no longer be separated from technological developments but must be integrated into the legal system.

This discussion also emphasizes the importance of a restorative justice approach in addressing cybercrime, particularly in cases involving individual harm. This approach allows for redress of victims' losses through compensation mechanisms or penal mediation, thus better fulfilling a sense of substantive justice. However, its application must be selective and consider the severity of the crime, so as not to reduce the deterrent effect on perpetrators. Furthermore, the discussion demonstrates that the reconstruction of criminal sanctions cannot be separated from institutional aspects and international cooperation. The transnational nature of cybercrime requires strong inter-institutional coordination and international cooperation. Therefore, strengthening the capacity of law enforcement officers through information technology and

digital forensics training is crucial. Furthermore, Indonesia also needs to expand international cooperation in cyber law enforcement, including in matters of extradition and data exchange.

Thus, this discussion confirms the interconnectedness of the three research questions and demonstrates that the criminal sanction system for cybercrime in Indonesia is still in a transitional stage. The new Criminal Code (KUHP) provides a progressive foundation, but it still requires strengthening and integration with other regulations to function optimally. The conceptual relevance of criminal sanctions is quite good, but their effectiveness is still limited by various structural and technical constraints. Therefore, reconstructing criminal sanctions is a strategic step to create a more adaptive, effective, and appropriate penal system to meet the challenges of cybercrime in the digital age.

Overall, this discussion leads to the conclusion that criminal law reform in Indonesia must continue, prioritizing cybercrime. Without comprehensive and integrative reconstruction, the existing criminal sanction system will struggle to keep pace with the increasingly complex and sophisticated developments in cybercrime. Therefore, a strong commitment is needed from legislators, law enforcement officials, and the public to collaboratively create a legal system capable of effectively and equitably addressing the challenges of the digital age. The implications of this research include both theoretical and practical implications. Theoretically, this research contributes to the development of modern criminal law studies, particularly in the context of adapting the criminal justice system to technology-based crimes. Practically, the results of this study can be used as a consideration by policymakers in formulating more comprehensive regulations related to cybercrime, and by law enforcement officials in optimizing the application of more effective and proportional criminal sanctions. Furthermore, this research also has implications for strengthening institutional capacity and increasing public digital literacy as part of a comprehensive cybercrime prevention strategy. Therefore, efforts to reform criminal law in Indonesia need to continue to be directed towards integrating norms, strengthening institutions, and utilizing technology to address the challenges of cybercrime in the digital era.

CONCLUSION

The conclusion of this study confirms that the construction of criminal sanctions for cybercrime in Law Number 1 of 2023 concerning the Criminal Code demonstrates a paradigm shift toward a more modern, flexible, and substantive justice-oriented criminal system through a double-track system approach. However, this construction remains general and does not explicitly regulate cybercrime offenses, so its implementation remains dependent on Law

Number 19 of 2016 concerning Electronic Information and Transactions. This situation creates a dualistic regulation that has the potential to hinder consistent law enforcement. In terms of relevance, the sanction system in the new Criminal Code conceptually aligns with the dynamic and complex characteristics of cybercrime. However, in terms of effectiveness, it remains suboptimal, as reflected in the increasing number of cybercrime cases not matched by an adequate level of resolution. This demonstrates that the effectiveness of criminal sanctions is determined not only by legal norms, but also by institutional capacity, technology, and coordination among law enforcement officials.

Furthermore, the ideal reconstruction of criminal sanctions for cybercrime needs to be directed towards an integrative and adaptive model, combining repressive, rehabilitative, and restorative approaches. Strengthening fines based on economic impact, implementing technology-based supervision, restricting digital access, and optimizing restorative justice mechanisms are strategic steps that can increase the effectiveness of punishment. Furthermore, harmonization between the new Criminal Code and the Electronic Information and Transactions (ITE) Law is an urgent need to create a criminal law system that is more integrated and responsive to technological developments.

The limitations of this research lie in its scope, which emphasizes a normative juridical approach supported by limited empirical data, thus not fully depicting the dynamics of law enforcement practices in the field comprehensively. Furthermore, limited access to sensitive cybercrime case data, which is not fully published, also hinders obtaining a more in-depth empirical picture. This research also does not specifically examine comparisons with the legal systems of other countries that are more advanced in handling cybercrime, so opportunities for enriching comparative perspectives remain open.

RECOMMENDATIONS

Based on the research findings, it is recommended that the government immediately reconstruct its cybercrime criminal sanction policy through a more adaptive and multidimensional approach, integrating progressive fines based on economic impact, digital surveillance for perpetrator rehabilitation, digital social work as a means of public education, restricting technology access as a preventative measure, and implementing restorative justice to ensure victim recovery. This is accompanied by strengthening regulations, increasing the capacity of technology-based law enforcement officers, cross-sector collaboration, and developing a transparent and sustainable digital-based evaluation and monitoring system. This

system can serve as a strategic reference for future researchers and stakeholders in formulating effective, responsive, and equitable policies in the digital era.

ACKNOWLEDGMENTS

The author expresses his gratitude to Allah SWT for the opportunity and health given to complete this research. He also thanks the Rector of Selamat Sri University, Central Java; the Rector of Al-Quran Science University, Central Java; the Rector of Balongan Indramayu Petroleum Technology Institute, West Java; the Vice Rectors 1, 2, and 3 of Selamat Sri University, Al-Quran Science University, Balongan Indramayu Petroleum Technology Institute; the Dean of the Faculty of Law of Selamat Sri University, Al-Quran Science University, Balongan Indramayu Petroleum Technology Institute, and fellow lecturers at Selamat Sri University, Al-Quran Science University, and Balongan Indramayu Petroleum Technology Institute for their moral and ethical support. He also thanks HORIZON: Indonesian Journal of Multidisciplinary for providing a platform for the publication of this research journal.

REFERENCES

Abdullah, A. Z., Fahira, J., & Rachmad, A. F. (2024). Kesadaran Hukum Pencegahan Cyberbullying dan Cyberpornography melalui Penguatan Informasi dan Regulasi Hukum pada Kalangan Gen-Z di Kota Pangkalpinang Fakultas Hukum Universitas Bangka Belitung, Indonesia Fakultas Hukum Universitas Bangka Belitung, Mela. *Jurnal Ilmu Hukum dan Tata Negara*, *2*(4). https://doi.org/https://doi.org/10.55606/birokrasi.v2i4.1557

Amarullah, A. H., Runturambi, A. J. S., & Widiawan, B. (2021). Analisis Ancaman Kejahatan Siber bagi Keamanan Nasional pada Masa Pandemi COVID-19. *Jurnal Kajian Stratejik Ketahanan Nasional*, *4*(2). https://doi.org/10.7454/jkskn.v4i2.10052

Audina, W. (2026). Kajian Yuridis Normatif terhadap Pengaturan Tindak Pidana Siber dalam Undang-Undang Informasi dan Transaksi Elektronik di Indonesia. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *4*(2), 7374–7386.

Butarbutar, J. M. (2025). Revolusi Digital dan Tantangan Kriminologis: Analisis terhadap Tren Kriminalitas dalam Era Digitalisasi. *Jurnal Media Hukum Indonesia*, *2*(6), 145–150.

Cahyono, S. T., Erni, W., & Hidayat, T. (2025). Reconstruction of Criminal Law Against Cybercrime in the Indonesian Criminal Justice System: Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia. *Dame Journal of Law*, *1*(1), 111–133

Daeng, Y., Levin, J., & Prayudha, M. R. (2023). Analisis Penerapan Sistem Keamanan Siber terhadap Kejahatan Siber di Indonesia. *Innovative: Journal of Social Science Research*, *3*(6), 1135–1145.

Hermawan, D. A., Putri, S. N., & Hosnah, A. U. (2025). Implementasi Regulasi Pidana dalam Melawan Kejahatan Siber pada Era Digital di Indonesia. *Journal of Innovative and Creativity*, *5*(3), 36877–36884.

Islami, Z. P. (2025). Tantangan Penegakan Hukum di Era Globalisasi Digital: Strategi Nasional Menghadapi Kejahatan Siber Lintas Batas. *AKSIOMA: Jurnal Sains Ekonomi dan Edukasi*, *2*(12), 2579–2591.

Kartadinata, A. (2026). Rekonstruksi Delik Pidana dalam Kejahatan Deepfake: Tantangan Pembuktian dan Perlindungan Korban. *Jurnal Ilmiah Ilmu Hukum dan Administrasi Publik*, *2*(1), 36–48.

Kresna, I. M., & Aditama, S. (2026). Pembaharuan Hukum Pidana di Indonesia: Analisis KUHP Baru dan Implikasinya. *Perspektif Administrasi Publik dan Hukum*, *3*(1), 11–19.

Maesaroh, R. S. (2024). Tantangan Keamanan Siber dan Implikasinya terhadap Hukum Kenegaraan: Tinjauan atas Peran Negara dalam Menjamin Ketahanan Digital. *Staatsrecht Jurnal Hukum Kenegaraan dan Politik Islam*, *4*(2).

Masri-zada, T., Martirosyan, S., Abdou, A., Barbar, R., Kades, S., Makki, H., Haley, G., & Agrawal, D. K. (2025). The Impact of Social Media & Technology on Child and Adolescent Mental Health. *HHS Pub Lic Access*, *9*(2), 111–130.

Megasari, I. I., & Azzahra, Y. H. (2025). Tantangan dan Kesiapan Menghadapi Ancaman Siber Indonesia. *Civic Education Perspective Journal*, *5*(2), 53–66.

Nurhakim, I., Sulastri, D., Kholik, M. A., & Muhammad, S. (2026). Perlindungan Hak Konstitusional Korban Kejahatan Siber melalui Hukum Pidana dalam Perspektif UUD 1945 dan Regulasi ITE. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *4*(3), 785–801.

Pamungkas, A. T., Muliyono, A., & Lahangatubun, N. (2024). The Crisis of Cybercrime Law Enforcement in Indonesia: Obstacles and Solutions. *DELICTUM: Jurnal Hukum Pidana Islam*, *2*(2), 149–162. https://doi.org/10.35905/delictum.v2i2.10613

Sani, R. R., Ghozi, W., Rafrastara, F. A., & Rahmawan, E. (2025). Penyuluhan dan Pelatihan Dasar Keamanan Siber pada Siswa SMK Muhammadiyah 1 Semarang. *JNPMIK (Jurnal Nasional Pengabdian Masyarakat Ilmu Komputer)*, *4*(2), 42–47.

Saputra, A., & Ismed, M. (2024). Rekonstruksi Penegakan Hukum Tindak Pidana Siber di Indonesia. *SEIKAT: Jurnal Ilmu Sosial, Politik dan Hukum*, *3*(1), 63–70.

Suryawin, P. C., Firdaus, M. R., Haryati, E., Rahim, A., & Randiana, P. (2026). Kajian Penegakan Hukum Tindak Pidana Cybercrime di Indonesia: Analisis Implementasi UU ITE dan Tantangan dalam Praktik. *Jurnal Realitas Hukum*, *2*(2), 145–158.

Wati, D. S., Nurhaliza, S., Sari, M. W., & Amallia, R. (2024). Dampak Cyber Crime terhadap Keamanan Nasional dan Strategi Penanggulangannya: Ditinjau dari Penegakan Hukum. *Jurnal Bevinding*, *02*(01), 44–55.