Journal of Cyber Law and Information Security
Volume 1, Number 2, 2022

Juridical Review of the Comparative Effectiveness of Cybercrime Criminal Law Enforcement (A Comparative Study of Indonesia and the United States)

Kuntadi[1*]

[1] Universitas Jendral Soedirman, Purwokerto, Indonesia

Abstract

The rapid advancement of information technology has led to the emergence of cybercrime, a form of crime characterized by its transnational nature, anonymity, and reliance on electronic systems. This study aims to analyze the effectiveness of cybercrime law enforcement in Indonesia and the United States using a normative comparative approach. In Indonesia, cybercrime is regulated under the Law on Information and Electronic Transactions (UU ITE), which governs various cyber offenses and their sanctions. However, its enforcement still faces challenges, including unclear legal provisions, limitations in handling electronic evidence, and the limited capacity of law enforcement officials. In contrast, the United States adopts a more specific and technical framework through the Computer Fraud and Abuse Act (CFAA), supported by integrated law enforcement institutions. This research employs a normative juridical method with a comparative law approach to examine both systems. The findings show that the effectiveness of cybercrime law enforcement is influenced not only by the existence of regulations but also by the clarity of legal norms, institutional strength, and the flexibility of the legal system in responding to technological developments.

Article history:
Received: September 18, 2022
Revised: October 29, 2022
Accepted: November 21, 2022
Published: December 30, 2022

Keywords:
Comparative Criminal Law, Computer Fraud and Abuse Act (CFAA), Cyber Legal Reform, Cybercrime Law Enforcement, Electronic Information and Transactions Law (UU ITE).

Identifier:
Zera Open
Page: 176-192
https://zeraopen.com/journal/jclis

*Corresponding author:
(Kuntadi)

©2022 The Author(s).
This is an open-access article under CC-BY-SA license (https://creativecommons.org/licence/by-sa/4.0/)

Therefore, regulatory strengthening and institutional reform are necessary to enhance cyber law enforcement in Indonesia so that it can better adapt to the evolving dynamics of digital crime.

1. Introduction

Digital transformation has brought fundamental changes to various aspects of modern society, including the social, economic, and legal spheres (Arianto, 2021). The rapid advancement of information and communication technology has fostered new patterns of interaction based on electronic systems and internet networks. Information technology no longer merely serves as a supporting tool for human activities; rather, it has become a primary infrastructure for the administration of government, economic transactions, public services, and business operations. While this massive digitalization offers significant benefits in terms of efficiency, speed, and ease of access to information, it also gives rise to complex and multidimensional legal consequences.

As society becomes increasingly dependent on digital technology, cyberspace has evolved into a new medium that is highly vulnerable to various forms of misuse. This development has given rise to new forms of crime that differ fundamentally from conventional criminal offenses. Cybercrime, or technology-based crime, is characterized by anonymity, transnational reach, and a high level of complexity, making law enforcement through conventional approaches increasingly challenging.

This condition places states in a position that requires adaptive legal responses capable of keeping pace with the evolving dynamics of crime in the digital sphere. In essence, cybercrime constitutes unlawful conduct committed through the use of computer systems, electronic networks, or digital data as the means, object, or target of criminal activity (Suhaemin & Muslih, 2021). In practice, the banking and digital finance sectors are among the most vulnerable to cybercrime, given their high economic value and the sensitivity of the personal data stored within electronic systems. Personal identity information, financial data, and authentication credentials are primary targets for cybercriminals seeking unauthorized access and exploitation. Consequently, cybercrime not only causes individual losses but also has systemic implications for economic stability, public trust, and national security.

In the Indonesian context, based on data from the National Cyber and Crypto Agency, the Minister of Communication and Information Technology, Johnny G. Plate, reported that between January and July 2021, Indonesia recorded 741,441,648 cyber threats. These threats encompassed various forms of cybercrime, including hacking, cracking, credit card fraud (carding), ATM skimming, phishing as a form of digital banking fraud, cybersquatting, the dissemination of malware such as viruses, bots, and worms, as well as offenses related to terrorism, human trafficking, and illegal online lending practices. These diverse forms of crime have become increasingly easy to perpetrate due to the widespread use of the internet and the rapid pace of technological advancement in the digital era (Parulian et al., 2021). This phenomenon prompted the Indonesian government to establish a specific regulatory framework through Law Number 11 of 2008 concerning Electronic Information

and Transactions, as most recently amended by Law Number 1 of 2016 (AS et al., 2021). However, in practice, the effectiveness of law enforcement against cybercrime continues to face criticism, particularly with regard to legal certainty, the protection of citizens' rights in the digital sphere, and the capacity and preparedness of law enforcement agencies to address cyber offenses that are technical in nature and cross jurisdictional boundaries.

The wide range of cybercrimes in Indonesia, including phishing, hacking, identity theft, malware distribution, and digital intimidation, demonstrates that cybercrime is a complex and multidimensional legal issue. Its consequences extend beyond financial losses to include reputational damage, psychological harm, and potential threats to national security and the stability of the digital economy. This condition indicates that the mere existence of regulations is insufficient without effective and equitable law enforcement.

On the other hand, the United States, as one of the pioneers in the development of information technology, demonstrates a comparatively more mature level of regulatory preparedness and cybercrime law enforcement. The U.S. legal system addresses cybercrime through various federal statutes that are both specific and adaptive, supported by coordinated enforcement policies involving law enforcement agencies and the private sector. This approach enables a faster and more effective response to the constantly evolving methods of cybercriminal activity.

Differences in regulatory frameworks, institutional capacity, and law enforcement practices between Indonesia and the United States make comparative

legal analysis a relevant and strategic approach. Through comparative study, weaknesses and gaps in Indonesia's cybercrime criminal law enforcement system can be identified, while also providing contextual normative lessons for legal reform. Based on this background, this study is formulated around two research questions: first, how effective are cybercrime regulations and criminal law enforcement in Indonesia compared to those in the United States; and second, why is the review and strengthening of cybercrime criminal law enforcement regulations a strategic urgency for Indonesia in addressing the evolving dynamics of global cybercrime?.

2. Methods

This study is a normative legal research project aimed at analyzing the effectiveness of the regulation and criminal law enforcement of cybercrime through a comparative legal approach. Normative legal research was chosen because the focus of the study is directed toward positive legal norms, legal principles, and legal doctrines governing cybercrime in both the Indonesian and United States legal systems. This approach is employed to assess the extent to which the objectives of regulatory formation align with their implementation in law enforcement practice, particularly in ensuring legal certainty, protecting citizens' rights, and enhancing the effectiveness of cybercrime prevention in the digital sphere.

The approaches used in this study include the statutory approach and the comparative approach. The statutory approach is used to examine the substance of cybercrime regulation within Indonesian legislation, as well as other relevant regulations within the criminal law system. Meanwhile, the comparative approach is

employed to compare the regulatory frameworks and law enforcement practices relating to cybercrime in Indonesia and the United States in order to identify similarities, differences, strengths, and weaknesses in each legal system.

The legal materials used in this study consist of primary, secondary, and tertiary legal sources. Primary legal materials include statutory regulations governing cybercrime, as well as relevant court decisions. Secondary legal materials comprise legal textbooks, scholarly journals, research findings, and other academic works discussing cybercriminal law and its enforcement. Tertiary legal materials are used as supporting references to clarify the legal concepts, terminology, and definitions applied in this research.

The collection of legal materials was conducted through library research by systematically identifying and reviewing various legal sources. The collected legal materials were then analyzed qualitatively using a descriptive-analytical method, which involves describing the applicable legal norms, evaluating the effectiveness of their implementation in law enforcement practice, and comparing them with the legal system of the United States. The results of this analysis are used to address the research questions and formulate normative and prescriptive conclusions.

3. Results & Discussion

3.1 The Effectiveness of Cybercrime Criminal Law Enforcement in Indonesia and the United States

The exponential development of information technology has created a new space for criminal activity characterized by its transnational nature, anonymity, and

reliance on electronic systems. Cybercrime has emerged as a logical consequence of society's increasing dependence on digital technology in various aspects of life, ranging from economic transactions, communication, and governmental administration to the management of strategic state data. Cybercrime possesses characteristics that fundamentally distinguish it from conventional crimes, commonly referred to as street crimes. Its emergence has been driven by advances in information technology, which were originally designed to facilitate and support human activities. As this technological revolution has progressed, patterns of social interaction have changed, particularly through the reduced need for direct physical interaction. The minimization of physical interaction is one of the defining features of the information technology revolution. In this context, social deviance has also adapted, giving rise to new forms of criminal behavior reflected in the patterns and methods of cybercrime. Consequently, electronic systems function not only as a medium for social activity but also as objects and instruments of crime vulnerable to exploitation by cybercriminals. This places the state under an obligation to establish a criminal law framework capable of providing effective protection for users of information technology while ensuring legal certainty in its enforcement.

In Indonesia, cybercrime is specifically regulated under Law Number 19 of 2016, which amended Law Number 11 of 2008 concerning Electronic Information and Transactions (the EIT Law). This legislation was designed to respond to the increasingly complex methods of cybercrime by broadening the scope of criminal offenses, clarifying the status of electronic evidence, and strengthening the authority of law enforcement agencies. In particular, Articles 27 through 35 of the EIT Law

regulate various forms of cybercrime (Agustian & Manik, 2021). Normatively, these provisions classify cybercrime into two main categories. First, cyber offenses that use electronic information as a means of committing unlawful acts, including online pornography, online gambling, defamation through social media, electronically based fraud, electronic forgery, extortion and threats through electronic media, dissemination of false information, copyright infringement, and cyberterrorism. Second, cyber offenses that target electronic systems, networks, and data, including illegal access, interference with electronic systems and data, unauthorized interception, electronic data theft, and the misuse of information technology devices. These provisions reflect the legislature's effort to address the dynamics and complexity of cybercrime by categorizing offenses based on both the means and the object of the crime. Criminal sanctions are set forth in Articles 45 through 52, including imprisonment and fines, with varying penalties depending on the seriousness of the offense and its consequences.

Nevertheless, the effectiveness of the EIT Law in practice continues to face structural and normative challenges. Several provisions have been criticized for containing vague and overly broad language, creating the potential for excessive criminalization, particularly in relation to freedom of expression in the digital sphere. These criticisms demonstrate that the mere existence of regulation does not necessarily guarantee effective law enforcement unless accompanied by clear legal norms, competent law enforcement personnel, and adequate technological infrastructure. Amendments to the EIT Law, including the state's authority to temporarily suspend access to accounts, bank accounts, and digital assets, were

intended to strengthen law enforcement's ability to reach cybercrime perpetrators (Kalensang et al., 2021).

In contrast, the United States adopts a more fragmented but technically precise and offense-specific regulatory approach. The principal legal framework for cybercrime enforcement in the United States is the Computer Fraud and Abuse Act, codified at 18 U.S.C. § 1030. The CFAA regulates in detail various forms of unauthorized access to protected computers, including illegal acquisition of data, computer fraud, damage to electronic systems, and cyber extortion. In addition, the United States has enacted several related federal statutes, including:

a. 18 U.S.C. § 1028 – Fraud and related activity in connection with identification documents, authentication features, and information. This provision criminalizes the unauthorized possession, production, storage, transfer, use, or trafficking of identification documents and authentication information. It bears similarities to forgery offenses under Indonesian criminal law. Violations are punishable by imprisonment ranging from five to thirty years, including attempts.

b. 18 U.S.C. § 1028A – Aggravated identity theft. This statute prohibits the unauthorized use, transfer, or possession of another person's identity or false identification documents. Violations carry a mandatory prison sentence of two to five years, without probation.

c. 18 U.S.C. § 1029 – Fraud and related activity in connection with access devices. This provision covers fraud involving access devices, including computer intrusion affecting both government systems and private individuals. Penalties range

from five to twenty years' imprisonment, with attempts punishable by five to ten years.

d. 18 U.S.C. § 1030 – Fraud and related activity in connection with computers. This provision governs fraud and offenses involving computer systems owned by both the government and private parties. Violations are punishable by imprisonment ranging from five to twenty years, while attempts may result in sentences of five to ten years.

e. 18 U.S.C. § 1037 – Fraud and related activity in connection with electronic mail. This statute criminalizes illegal conduct involving electronic mail, including sending emails through hijacked computers, falsifying sender identities, and using false information to gain access to email systems. Violations are punishable by up to three to five years' imprisonment.

f. 18 U.S.C. § 1343 and 18 U.S.C. §§ 1466A, 2251, and 2252 – These provisions regulate wire fraud and child pornography offenses. They prohibit the production, distribution, possession, and receipt of child sexual exploitation materials in any medium, carrying severe penalties ranging from five to forty years' imprisonment, and in some cases life imprisonment, including for attempts.

The effectiveness of cybercrime law enforcement in the United States is further supported by an integrated and highly professional institutional framework. Cybercrime cases are handled not only by conventional law enforcement agencies but also by specialized institutions such as the Federal Bureau of Investigation, the United States Department of Justice, and the Cybersecurity and Infrastructure Security Agency, all of which play strategic roles in the prevention, investigation, and

prosecution of cybercrime. Additionally, the U.S. criminal justice system recognizes plea bargaining, which enables cooperation between offenders and law enforcement authorities to uncover broader cybercriminal networks. Thus, the effectiveness of enforcement is measured not solely by the severity of sanctions, but also by the successful dismantling of organized cybercrime.

In Indonesia, cybercrime enforcement also involves the roles of virtual police and cyber police, each operating at different stages of authority. Virtual police are tasked with educating the public and issuing warnings regarding compliance with the EIT Law. Cyber police, by contrast, perform law enforcement functions when violations cannot be resolved through the persuasive and preventive measures undertaken by virtual police. Accordingly, virtual police serve as a preventive mechanism at the initial stage, before matters are escalated to formal investigation by cyber police. However, the concept of virtual police remains relatively new and is not yet fully understood by the public. Although the Indonesian National Police previously maintained cyber units with similar functions, the distinction between virtual police and cyber police is still not widely recognized, partly due to limited public education efforts. As noted by Sari (2021), virtual police focus primarily on prevention, while cyber police directly exercise investigative and enforcement powers under applicable law.

A comparison between Indonesia and the United States demonstrates that the effectiveness of cybercrime law enforcement is determined not only by the existence of regulations, but also by the quality of legal drafting, evidentiary systems, institutional capacity, and the flexibility of criminal law mechanisms. Indonesia

continues to face challenges in balancing human rights protection with the need for firm cyber law enforcement, whereas the United States has a comparative advantage in technical and institutional aspects, despite ongoing criticism regarding the expansive scope of the CFAA. These differences provide an important basis for evaluating the effectiveness of each legal system in responding to the ever-evolving dynamics of cybercrime.

3.2 The Urgency of Strengthening Cybercrime Regulation and Law Enforcement in Indonesia

The urgency of strengthening cybercrime regulation and law enforcement in Indonesia cannot be separated from the dynamic, transnational, and rapidly evolving nature of cybercrime, which often develops faster than the formation of positive legal norms. From a legal perspective, particularly criminal law, cybercrime presents a highly urgent issue that must be addressed effectively and systematically. Cybercrime has evolved beyond conventional forms of criminality into technologically sophisticated offenses characterized by cross-jurisdictional operations and anonymity. This evolution has exposed a significant gap between the realities of cybercrime and the existing criminal law framework. Various studies indicate that Indonesia's criminal law system, whether under the Criminal Code or the EIT Law, has not yet fully addressed contemporary forms of cybercrime, particularly those involving attacks on electronic systems, large-scale data manipulation, and offenses targeting national digital infrastructure.

In practice, the development of cybercrime in Indonesia has shown escalation not only in quantity but also in quality. Cybercrime methods are no longer limited to

simple fraud or conventional hacking; they have evolved into organized criminal activities involving large-scale data manipulation, attacks on digital infrastructure, and the systematic exploitation of digital identities. This demonstrates that cybercrime has transformed into a threat to digital economic stability, national security, and state data sovereignty.

The urgency of strengthening cybercrime law enforcement is also closely related to the evolving paradigm of modern criminal law, which must be increasingly adaptive in addressing new forms of criminal conduct (Habibi & Liviani, 2020). Cybercrime poses serious challenges in evidentiary processes, the tracing of electronic evidence, and the determination of legal responsibility, especially when perpetrators operate across borders and employ identity-concealment technologies. Therefore, Indonesian criminal law must be developed adaptively to respond effectively to these new forms of criminality, rather than remaining confined to classical territorial and conventional evidentiary approaches. Without such a paradigm shift, the criminal justice system risks losing its capacity to respond to the continuing transformation of digital technology.

From the perspective of criminal policy, strengthening cybercrime regulation must also be carried out proportionally and carefully. The regulation of cyber offenses should not lead to overcriminalization, as this could hinder the development of information technology and the digital industry, both of which are strategically important for Indonesia in the global competitive landscape. Accordingly, the criminalization of cybercrime should adhere to at least three fundamental principles. First, the principle of selectivity and limitation, meaning that

only conduct causing serious harm and threatening protected legal interests should be criminalized. Second, the principle of cost and benefit, which requires that the costs of drafting regulations, monitoring compliance, and enforcing the law including the need for advanced technological infrastructure be proportionate to the legal and protective benefits achieved. Third, the principle of enforcement capacity, which requires that law enforcement personnel possess sufficient expertise and resources so that enacted norms do not become merely symbolic rules that are difficult to implement in practice.

Compared with the United States, the fundamental differences lie not only in regulation but also in institutional design and criminal policy approaches. The United States treats cybercrime as a matter of national security, addressed through cross-sectoral coordination involving specialized agencies such as the Federal Bureau of Investigation, the United States Department of Justice, and the Cybersecurity and Infrastructure Security Agency, supported by a highly specific and technical legal framework through the CFAA and other federal regulations. This approach enables faster, more measured, and better-coordinated responses to evolving cyber threats. By contrast, cybercrime enforcement in Indonesia remains distributed across multiple institutions, with coordination that is not yet fully optimal. As a result, the effectiveness of enforcement often depends heavily on the sectoral capacity of each institution.

From the perspective of criminal law policy, this condition demonstrates that strengthening cybercrime regulation in Indonesia cannot be achieved merely through legislative amendment. It must also be accompanied by systemic reform of

the law enforcement structure. Such strengthening should include regulatory harmonization, enhancement of the technical capacity of law enforcement personnel, and the development of more effective mechanisms for international cooperation in addressing transnational cybercrime. Without comprehensive reform, Indonesia's cybercrime legal framework risks losing its responsiveness to the rapid pace of technological development.

4. Conclusion

Based on the analysis of the effectiveness of cybercrime criminal law enforcement in Indonesia and the United States, it can be concluded that the development of cybercrime has posed serious challenges to modern criminal justice systems. The transnational, technology-based, and conventionally difficult-to-trace nature of cybercrime means that criminal law can no longer rely solely on traditional approaches; instead, it must be adaptive and responsive to the rapid evolution of digital technology.

In Indonesia, cybercrime has been regulated *Undang-Undang Nomor 1 Tahun 2016 amandement Undang-Undang Nomor 8 Informasi dan Transaksi Elektronik (UU ITE).* This legislation provides a fairly comprehensive legal framework for addressing various forms of cybercrime, both those that use electronic systems as a means of committing offenses and those that target electronic systems as the object of criminal activity. Nevertheless, its implementation continues to face several challenges, including the lack of clarity in certain legal provisions, the potential for multiple interpretations, and the complexity of electronic evidence in criminal proceedings.

In addition, the limited technical capacity of law enforcement officials and insufficient inter-agency coordination have affected the overall effectiveness of cybercrime law enforcement in Indonesia.

By contrast, the United States demonstrates a more systematic and technically sophisticated approach to combating cybercrime through the Computer Fraud and Abuse Act and various other federal regulations. More specific legal provisions concerning criminal conduct provide greater legal certainty and facilitate more effective enforcement. This effectiveness is further strengthened by the presence of integrated law enforcement institutions such as the Federal Bureau of Investigation, the United States Department of Justice, and the Cybersecurity and Infrastructure Security Agency, which work synergistically to address cybercrime. Moreover, the plea bargaining mechanism provides additional flexibility in uncovering broader criminal networks.

Accordingly, it can be firmly asserted that the effectiveness of cybercrime law enforcement is determined not merely by the existence of regulations, but also by the quality of legal drafting, institutional capacity, and the flexibility of the legal system in responding to technological developments. Indonesia still requires significant strengthening in both its normative and institutional frameworks to ensure more effective cybercrime law enforcement, greater legal certainty, and optimal protection for society in the digital sphere amid the continuing dynamics of digital transformation.

References

Agustian, R. A., & Manik, J. D. N. (2021). *Tindak pidana informasi elektronik dalam kerangka hukum positif*. PROGRESIF: Jurnal Hukum, 15(1), 92–111.

Arianto, B. (2021). *Pandemi Covid-19 dan transformasi budaya digital di Indonesia*. Titian: Jurnal Ilmu Humaniora, 5(2), 233–250.

AS, M. W., Wiryawan, I. W. G., & PP, K. S. L. (2021). *Faktor penyebab terjadinya kejahatan cyber crime yang dilakukan oleh orang asing di Bali ditinjau dari perspektif kriminologi*. Jurnal Yusthima, 1(1), 58–70.

Habibi, M. R., & Liviani, I. (2020). *Kejahatan teknologi informasi (cyber crime) dan penanggulangannya dalam sistem hukum Indonesia*. Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam, 23(2), 400–426.

Kalensang, R., Soepeno, M. H., & Karwu, G. M. F. (2021). *Tinjauan yuridis efektivitas Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik*. Lex Crimen, 10(4), 205–214.

Parulian, S., Pratiwi, D. A., & Yustina, M. C. (2021). *Studi tentang ancaman dan solusi serangan siber di Indonesia*. Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT), 1(2), 85–92.

Sari, U. I. P. (2021). *Kebijakan penegakan hukum dalam upaya penanganan cyber crime yang dilakukan oleh virtual police di Indonesia*. Journal of Studia Legalia, 2(1), 58–77.

Suhaemin, A., & Muslih, M. (2021). *Karakteristik cybercrime di Indonesia*. EduLaw: Journal of Islamic Law and Jurisprudence, 2(1), 15–26.