Discourse journal on Law and Society

E-ISSN: 3089-6797
P-ISSN: 3089-6789

Research Article

The Development of Cybercrime as a Criminal Offense in the Digital Era and Its Impact on Society

Tagor Aruan[1]*, Rahmayanti[2]

[1] Universitas Pembangunan Panca Budi, Indonesia; e-mail : tagoraruan@surveyorclub.com
[2] Universitas Pembangunan Panca Budi, Indonesia; e-mail : rahmayanti@dosen.pancabudi.ac.id
* Corresponding Author : Tagor Aruan

Abstract: The development of information technology has brought about significant changes in the social, economic, and legal life of global society. On the one hand, digitalization creates efficiency and convenience in various activities, such as financial transactions, communications, and access to information. However, on the other hand, this progress has also given rise to a new form of crime known as cybercrime. Cybercrime differs from conventional crime in that it is committed through electronic systems that can cross national borders and involve a large number of victims. This crime encompasses various forms, such as data hacking, online fraud, and malware distribution. This research aims to examine the development of cybercrime as a form of modern crime in the digital era and to assess the response of Indonesian criminal law to these challenges. The method used is normative legal, with a statutory, conceptual, and case study approach. This research also examines existing regulations, such as Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) and Law Number 27 of 2022 concerning Personal Data Protection, in addressing cybercrime issues. The research results show that although Indonesia has several regulations related to cybercrime, their implementation still faces various obstacles. Some of the main obstacles include suboptimal law enforcement, limited technology and human resources, and low levels of public digital awareness. Therefore, regulatory reform, institutional capacity development, and increasing public digital literacy are essential. This is part of a national strategy to address cybercrime comprehensively and sustainably, in order to create a safer and more trustworthy digital environment.

Keywords: criminal law, cyber crime, cybercrime, digitalization, information technology.

1. Introduction

The development of information and communication technology in the digital era has had a major impact on various aspects of human life, including in terms of social, economic and government interactions. Rapid digital transformation brings many conveniences, such as efficiency in public services, ease of transactions, and acceleration of information flow. However, behind this progress, new challenges have also emerged in the form of increasingly complex and transnational cyber crime. Cyber crime is a form of crime that utilizes digital technology as the main means of committing criminal acts. This crime is no longer limited by time and space, and can target anyone, from individuals, corporations, to the state. The forms are increasingly diverse, such as hacking, theft of personal data, spreading hoaxes, online fraud, and digital -based sexual exploitation. These crimes are often difficult to detect, track, and take legal action against because the perpetrators can be outside the jurisdiction of the victim's country. Indonesia as a developing country is also not immune to the negative impacts of cybercrime. The increasing use of the internet and the digitalization of public services have opened new loopholes for criminals to commit criminal acts through cyber networks. Data from various institutions show a significant increase in cybercrime cases every year, such as digital fraud, illegal access to electronic systems, and violations of personal data protection. Although Indonesia has regulations governing cybercrime, such as Law No. 11/2008 on Electronic Information and Transactions (UU ITE) and its amendments, as well

Received: 11 June, 2025
Revised: 19 July, 2025
Accepted: 02 August, 2025
Published: 04 August, 2025
Curr. Ver.: 04 August, 2025

as Government Regulations and Ministerial Regulations related to cybersecurity and data protection, there are still many challenges in law enforcement. Problems such as overlapping regulations, limited law enforcement officers in terms of digital capacity, and lack of public awareness of digital security are the main obstacles.

Cyber crime in the digital era is not only a legal issue, but also a national issue that impacts the security, economy and sovereignty of the state. Therefore, it is necessary to conduct a comprehensive assessment of the development of cyber crime and how criminal law is able to respond to these dynamics effectively and adaptively. This research is important to review the role of law in dealing with cybercrime and encourage the renewal of regulations and law enforcement systems that are responsive to the challenges of digitalization. Apart from the rapid growth of information technology, the development of cyber crime is also influenced by the increasing dependence of society on electronic systems. Almost all sectors of life including government, banking, education, and health services have switched to digital systems. This condition creates a new space that is very vulnerable to abuse by irresponsible parties. The ease of accessing the internet network is not only utilized for positive activities, but also opens up opportunities for the emergence of new criminals with methods that are no longer conventional. Various cases of crimes such as phishing, malware, digital extortion (ransomware), distribution of illegal content, and online child exploitation are now becoming global concerns. In Indonesia, a number of emerging cyber cases such as the theft of e-commerce customer data, attacks on government systems, and the rise of hoax content ahead of the election, show that cybercrime is not just a technical crime, but can damage social stability and democracy. The losses incurred are not only economic, but also psychological, social, and even ideological.

Criminal law as an instrument of public protection faces challenges in responding to this development. The borderless, anonymous, and dynamic characteristics of cybercrime mean that positive law often lags behind the modus operandi of the perpetrators. Therefore, a progressive, adaptive and technology-based legal approach is needed. Furthermore, synergy between policymakers, law enforcers, and other stakeholders is needed to create a legal ecosystem that is able to answer the challenges of the digital era. Collaboration between countries is also important, considering that cybercrime does not recognize national jurisdictional boundaries. Through international cooperation and national regulatory reform, it is hoped that Indonesia's legal system can provide effective legal protection while providing a deterrent effect against cyber criminals. Taking into account the urgency and complexity of the problem, an in-depth study of the development of cyber crime as a new form of crime in the era of digitalization is important. This study is not only academically relevant, but also very strategic for the formulation of criminal law policies in the future..

2. Literature Review

Definition

Cyber crime is any form of crime committed by utilizing information and communication technology, especially internet networks and electronic devices. According to the United Nations Office on Drugs and Crime (UNODC), cyber crime includes two main categories:

- Computer-related crime, which is conventional crime committed with the help of computers.
- Computer crime, which is a crime that can only occur because of computer technology, such as hacking or malware attacks.

In the context of Indonesian law, this term is not explicitly defined in Law Number 11/2008 on Electronic Information and Transactions (UU ITE), but various acts classified as cyber crime have been regulated in certain articles, for example regarding illegal access, online defamation, electronic data manipulation, and so on.

Criminal Law Approach

In criminal law, cybercrime can be studied from two angles:

- Substantive Aspect

Related to the formulation of offenses in legislation. The ITE Law is the main basis for regulating cyber crimes in Indonesia, but several articles in the Criminal Code can also be applied subsidiarily.

- Formil/Procedural Aspects

Concerning how the investigation, prosecution, and trial of cyber crimes are conducted. Challenges arise because electronic evidence has special characteristics, such as being easily altered or deleted.

- Sociological Aspect

Law enforcement against cybercrime must consider the social conditions, digital culture of the community, and the readiness of human resources in law enforcement officials.

Urgency of Study

The study of the development of cyber crime is very important considering that this crime not only threatens individuals, but also institutions and even the state. Without adequate theoretical studies, efforts to overcome cyber crime will always lag behind the dynamics of the crime itself. Therefore, a theoretical approach becomes an important foundation to formulate a comprehensive and adaptive legal strategy for the digitalization era.

3. Proposed Method

The research method used in this study is normative legal research or doctrinal research. Normative legal research is conducted by examining relevant laws and regulations, legal doctrines, and the views of experts to understand and analyze how criminal law responds to the development of cyber crime in the era of digitalization. This type of research emphasizes the study of written legal norms, without collecting field data. This research uses several approaches, namely the statutory approach, conceptual approach, and case approach. The statutory approach is used to examine various regulations governing cyber crimes, such as Law Number 11/2008 on Electronic Information and Transactions and its amendments, as well as provisions in the Criminal Code. The conceptual approach is used to examine basic concepts such as cyber crime, digitalization, and legal protection in criminal law. Meanwhile, the case approach is carried out by analyzing court decisions related to cyber crime that have been decided by national and international courts. The legal materials used in this research consist of primary, secondary, and tertiary legal materials. Primary legal materials include legislation and court decisions that are directly related to the object of research. Secondary legal materials include legal literature, scientific journals, scientific works of lecturers or legal experts, as well as publications from authorized institutions such as the State Cyber and Crypto Agency (BSSN) or the Ministry of Communication and Information. Meanwhile, tertiary legal materials are supporting materials such as legal dictionaries and encyclopedias used to explain legal terms used in research.

4. Results and Discussion

The development of digital technology has created major changes in the way humans interact, transact and carry out social activities. Digitalization has touched almost all sectors, from government, education, trade, to financial services. Behind these benefits, there are also negative impacts in the form of increasing cyber crime, which poses a serious challenge to national and international legal systems. Cyber crime is growing along with the sophistication of information technology. Crimes that used to be committed physically can now be committed without having to meet the victim face-to-face, and even remotely through the internet. This phenomenon makes cybercrime a modern form of crime that is transnational, anonymous, and difficult to trace. The types of cybercrime that often occur in Indonesia include personal data theft, online fraud, account and system hacking, illegal content distribution, and electronic-based sexual crimes. In the Indonesian context, cybercrime is specifically regulated in Law Number 11/2008 on Electronic Information and Transactions (ITE Law), which was later updated with Law Number 19/2016. This law is the main legal basis in ensnaring cyber criminals. In addition, some provisions in the Criminal Code are also still used simultaneously, especially in cases that have conventional criminal elements, such as fraud and defamation. Despite having a legal basis, the enforcement of cybercrime still faces various obstacles. First, the cross-jurisdictional nature of cybercrime often makes it difficult for law enforcement officials to track down perpetrators who are located abroad. Second, the lack of human resource capacity in the field of digital forensics is also an obstacle in the evidentiary process. Third, the mismatch between technological developments and the speed of regulatory updates causes many new actions in the digital world to not have an adequate legal basis. In addition, the aspect of protection for victims of cybercrime is also still less than optimal. Many victims of online fraud or data theft do not receive maximum legal protection, and some do not even report it because they feel they will not get justice. This shows that the

criminal law system has not been fully adaptive to the changing digital crime landscape. Cyber crime not only affects individuals, but also threatens state security and social stability. Attacks on government digital systems, critical infrastructure, and financial institutions can cause huge losses, both economically and reputationally. Therefore, it is important for Indonesia to continue to strengthen the national legal system through updating laws and regulations, increasing the capacity of law enforcement officers, and strengthening international cooperation in the field of cyber security. From a criminal law perspective, cyber crime is a new challenge that demands a progressive legal approach. Law does not only function as a means of punishment, but also as a means of prevention and protection. Therefore, the development of criminal law in the future must consider the dynamics of the digital world, and be able to create legal instruments that are preventive, repressive, and corrective.

Thus, the development of cyber crime in the digitalization era shows that criminal law must be able to transform along with technological advances. Handling cybercrime is not enough only through prosecution, but also requires public education, the establishment of responsive regulations, and collaboration between the government, society, and the private sector in creating a safe and equitable digital space. The development of cyber crime cannot be separated from the social factors and digital culture of the society. Many internet users in Indonesia do not have adequate digital literacy, especially in terms of personal data security, digital ethics, and understanding of cyber threats. This lack of awareness is utilized by cyber criminals to carry out various modes of online fraud, such as phishing, social engineering, and spreading links containing malware. The public is often victimized not only because of negligence, but also because of the weak digital protection system available to the public. In the dimension of criminal law, cyber crime has unique characteristics that distinguish it from conventional crime. One of them is the form of attack that is not always physically visible. A perpetrator can commit a crime from abroad without directly touching the object or victim.

This poses a jurisdictional challenge, namely how a country can prosecute a perpetrator who is outside its jurisdiction. This is what causes the need for cross-border legal cooperation or mutual legal assistance in processing international cyber crime perpetrators. In addition, the problem of proof in cyber cases is also a crucial aspect. Electronic evidence is easily modified, copied, or deleted. Therefore, law enforcement officials must have adequate digital forensic capabilities and technological support tools. The investigation process requires caution and speed in handling digital evidence so that it remains legally valid and can be accounted for in court. On the other hand, the development of criminal law in responding to cybercrime is also influenced by public and media pressure. Many cyber cases that have attracted widespread public attention - such as doxing, spreading hoax content, online hate speech, and spreading immoral content - have prompted the government to respond immediately through regulations. However, responding too quickly without in-depth studies also risks creating new problems, such as multiple interpretations of articles and potential violations of the right to freedom of expression. For example, the application of Article 27 paragraph (3) of the ITE Law on defamation through electronic media often draws criticism because it is considered vulnerable to abuse to silence public criticism or criminalize citizens.

Therefore, it is important to maintain a balance between legal certainty, protection of victims, and respect for human rights in law enforcement against cybercrime. Meanwhile, at the policy level, Indonesia has also taken strategic steps such as establishing the State Cyber and Crypto Agency (BSSN) and encouraging the enactment of new regulations such as the Personal Data Protection Law (PDP Law). The presence of the PDP Law is an important milestone in providing legal certainty for the rights to citizens' personal data, which has been prone to exploitation in the digital space. However, the establishment of regulations is not enough. Continuous efforts are needed in the form of digital education to the public, training of law enforcement officers, strengthening IT security systems in government and private institutions, and acculturating healthy digital ethics in the community. Criminal law must be a tool that not only punishes, but also prevents and protects the public interest in an increasingly open digital space. By considering all of the above aspects, it can be concluded that cybercrime is a complex and fast-growing form of modern crime, along with the advancement of information technology. Criminal law as a means of social control must adapt, both in terms of legal substance, institutions, and law enforcement approaches. The response to cybercrime cannot be done partially, but must be through an integrated and collaborative national strategy, both at the national and international levels.

5. Conclusions

The development of information technology in the digital era has brought convenience and acceleration in various aspects of life. However, this progress has also created new challenges in the form of cyber crime, which is increasingly complex and difficult to control. Cyber crime is a modern form of crime that utilizes digital technology as the main means, with cross-border characteristics, physical intangibility, and great destructive power. In Indonesia, cybercrime has increased significantly in line with the increase in community activities in the digital space. These crimes include various forms, such as online fraud, hacking, data theft, and spreading illegal content. Although the government has responded through various regulations, such as the Electronic Information and Transaction Law (ITE Law) and the Personal Data Protection Law (PDP Law), there are still various obstacles in its implementation and enforcement. Some of the obstacles faced include limited jurisdiction, weak technical capacity of law enforcement officials, not optimal digital literacy of the community, and overlapping or multiple interpretations of articles in existing regulations. Criminal law as a means of social control is required to be adaptive and progressive in responding to digital crime. A legal approach that is too repressive without contextual understanding can have a counterproductive impact on freedom of expression and the protection of human rights. Therefore, a balance between legal certainty is needed.

In response to the increasing complexity of cyber crime in the digitalization era, comprehensive and sustainable efforts are needed from various parties, especially the government and law enforcement officials. An important first step is to update criminal law regulations to be in line with the development of information technology. Existing regulations, such as the Electronic Information and Transaction Law and the Personal Data Protection Law, need to be harmonized and clarified so as not to cause multiple interpretations and be able to provide legal certainty for the digital community. Through a comprehensive, collaborative and responsive law-based strategy, Indonesia can strengthen legal resilience in the face of cybercrime and create a safe, just and sovereign digital space.

References

[1] Arief, B. N., *Problems of Law Enforcement and Criminal Law Policy in Crime Control*, Jakarta: Kencana, 2016.

[2] State Cyber and Crypto Agency (BSSN), *Annual Report on National Cyber Security*, Jakarta: BSSN, 2022. Accessed from https://bssn.go.id

[3] Effendi, M., "Cybercrime and Law Enforcement in Indonesia," *Journal of Law and Development, 51*(1), pp. 105-120, 2021. https://doi.org/10.21143/jhp.vol51.no1.2763

[4] Harjono, A., *Cybercrime and the Urgency of Law Reform in the Digital Age*, Yogyakarta: Genta Press, 2020.

[5] Ministry of Communication and Information of the Republic of Indonesia, *Cyber Crime Trends and Control Strategies*, Jakarta: Directorate General of Informatics Applications, 2023. Accessed from https://kominfo.go.id

[6] Marzuki, P. M., *Legal Research: A Practical Approach*, Jakarta: Kencana, 2005.

[7] Nugroho, Y., *Towards Democratic Cybersecurity Governance in Indonesia*, Jakarta: Center for Innovation Policy and Governance (CIPG), 2018.

[8] Pratama, P. A., "Cyber Crime in the Perspective of Criminal Law and its Future Challenges," *Journal of Actual Legal Science, 7*(2), pp. 45-59, 2023.

[9] Susanto, H., *Cybersecurity and Cyberwar: A Legal and Strategic Approach*, Bandung: Refika Aditama, 2019.

[10] Law Number 11 of 2008 concerning Electronic Information and Transactions, *State Gazette of the Republic of Indonesia*, Year 2008, Number 58.

[11] Law Number 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions, *State Gazette of the Republic of Indonesia*, Year 2016, Number 251.

[12] Law No. 27 of 2022 on Personal Data Protection, *State Gazette of the Republic of Indonesia*, Year 2022, Number 182.

[13] UNODC, *Comprehensive Study on Cybercrime*, United Nations Office on Drugs and Crime, 2013. https://www.unodc.org/documents/organized-crime/

[14] Wijayanto, A., "Regulation and Protection of Personal Data in the Digital Era: A Juridical Review of Digital Consumer Protection," *Journal of Indonesian Legislation, 19*(3), pp. 233-248, 2022.

[15] Choi, J., "Cybercrime and its impact on the digital economy," *Journal of Digital Security, 3*(2), pp. 45-61, 2019. https://doi.org/10.1016/j.jds.2019.01.005