JURIDICAL REVIEW OF INFORMATION TECHNOLOGY CRIME (CYBERCRIME) AND THE APPLICATION OF INDONESIAN CYBERLAW

Afifah Nur Rahmawati[1]

Abstract

This research examines information technology crimes (cybercrime) and the implementation of cyberlaw in Indonesia. With the increasing use of internet and digital technology, cyber crimes have become a serious threat requiring effective legal handling. This study employs a qualitative method with a literature study approach to analyze various aspects of cybercrime and cyberlaw implementation. The research aims to provide a comprehensive overview of cybercrime forms in Indonesia, evaluate the effectiveness of existing regulations, and analyze the role of stakeholders in implementing cyberlaw. Through literature studies encompassing academic articles, legal documents, and government reports, this research systematically examines the development and implementation of cyber regulations in Indonesia. The results show that cybercrime takes various forms, including cyberterrorism, cyber-pornography, cyber-harassment, hacking, and carding. The implementation of cyberlaw in Indonesia is regulated through the ITE Law No. 11 of 2008 and PDP Law, involving various stakeholders such as government, law enforcement, private sector, and society. This research concludes that strong cooperation between stakeholders and increased public awareness are necessary to create a secure digital environment

Keywords: Cybercrime, Cyberlaw, *ITE* Law

INTRODUCTION

The development of the times in the era of globalization affects the development of information and communication technology which is increasing rapidly. In recent years, the development of information and communication technology in Indonesia has made significant progress, in line with the increase in internet access and the use of digital devices. According to data from the Indonesian Internet Service Providers Association (APJII), the number of internet users in Indonesia continues to increase, reaching more than 200 million people in 2023. This has an influence on the way humans interact, do business, and socialize in daily life. With increasingly advanced technology, people are promised easy access and wider access to the world market.

Information Technology is considered an important aspect in spurring the growth of the world economy. In fact, there are two things that are considered beneficial for the world economy. First, technology drives demand related to information technology products such as computers, modems, and internet networking equipment. Second, it is to facilitate business transactions, including business finance or finance. However, behind the convenience offered by the existence of advanced technology, there are also challenges and threats, one of which is information technology crime or cybercrime. Thus, there is a positive impact and there is also a negative impact of the development of information technology, so it is called a double-edged sword.[2]

Cybercrime refers to criminal acts committed by utilizing information technology and the internet. Cybercrime or in the Indonesian Wikipedia calls it

[1] Master of Law Student of Surabaya State University, email: 24131585008@mhs.unesa.ac.id

[2] Ahmad Ramli, Cyber Law and IPR in the Indonesian Legal System (Bandung: Rafika Aditama, 2019), p.1.

Cybercrime, which means a crime involving computers and networks.[3] Cybercrime encompasses different types of crimes committed through digital media, such as online fraud, identity theft, hacking, malware spread, and the spread of illegal content. According to an annual report from the State Cyber and Cryptography Agency (BSSN), the number of cybercrime cases in Indonesia has increased exponentially in recent years, creating concern among the government, the public, and business people. These threats not only harm individuals but can also disrupt economic stability and national security. The forms of crime in the development of technology are very diverse, there are many new crimes such as data manipulation, espionage, provocation, money laundering hacking, etc. The pace of crime in the internet network is difficult to follow with the government's ability to balance and control.[4]

The Indonesian government is not silent without any action to overcome this cybercrime. The Electronic Information and Transaction Law was made which was passed by the House of Representatives on March 25, 2008. This proves that Indonesia is not left behind other countries in overcoming cybercrime by making legal tools in the field of Cyber space law. This law includes cyberlaw in Indonesia which discusses the broad scope of cyber regulations.[5] The birth of the Law, it is hoped that it can be a concrete answer to the problems faced by law enforcement officials. Based on the phenomenon that has occurred that has been described above, the author is encouraged to conduct a research entitled "Juridical Review of Information Technology Crime (Cybercrime) and the Application of Cyberlaw in Indonesia".

METHOD

This research uses a Qualitative approach. The choice of a qualitative approach method is because the author can explore the phenomenon dynamically and study with the applicable juridical regulations. Data collection is carried out through a literature review that includes a variety of sources, such as books, scientific articles, and official reports from government agencies and non-governmental organizations. This literature study aims to identify relevant theories and applicable legal frameworks related to cybercrime and cyberlaw in Indonesia. In addition, secondary data from previous research was also analyzed to provide broader context regarding the problems faced in handling cybercrime. After the data is collected, the data analysis is carried out descriptively and thematically. The researcher categorizes the information based on the type of cybercrime, the challenges faced in law enforcement, and the effectiveness of existing regulations. This analysis aims to identify the patterns that emerge from the data, as well as formulate arguments that support the research findings.

Through this research method, it is hoped that it can provide efficient and accurate research results with the phenomenon that occurs, as well as make a significant contribution to the development of the academic field and public policy in Indonesia. This research aims to provide constructive and accountable recommendations for

[3] "Cybercrime - Wikipedia Indonesian, The Free Encyclopedia," accessed October 23, 2024, https://id.wikipedia.org/wiki/Kejahatan_siber.

[4] Markus Djarawula, Novita Alfiani, and Hanita Mayasari, "Juridical Review of Information Technology Crimes (Cybercrime) in Indonesia Reviewed from the Perspective of Law Number 11 of 2008 concerning Information and Electronic Transactions," Journal of Scientific Horizon 2, no. 10 (2023): 3799–3806.

[5] Riko Nugraha, "Indonesian Legal Perspective (Cyberlaw) Handling Cyber Cases in Indonesia," Aerospace Law Scientific Journal Vol 11 No. (2021), p.20.

policymakers and law enforcement agencies, trying to foster and increase public awareness of the importance of handling cybercrime, By understanding the existing context and challenges, it is hoped that more effective measures can be implemented to deal with the threat of cybercrime in the digital era. In addition, this research also aims to provide a comprehensive overview in general of the forms of cybercrime that occur in Indonesia and the effectiveness of the implementation of existing regulations.[6]

RESULTS AND DISCUSSION

Basic Concepts of Cybercrime

Cybercrime Review is a term used to describe various types of crimes committed through or against computer systems and networks that include illegal activities involving computers as tools, targets, or storage of evidence of crimes. The definition of Cybercrime in ITE Law Number 11 of 2008 defines that cybercrime or electronic crime is an attempt to enter and/or use computer network facilities without permission and unlawfully with or without causing changes and/or damage to the computer facilities used.

The definition of the concept of cybercrime according to the U.S. Dept. of Justice states that cybercrime is any illegal act that requires literacy about computer technology for malicious acts, investigations, or prosecutions. Meanwhile, according to Andi Hamzah, Cybercrime is a crime committed by internegt networks and computers that are generally carried out by computer users illegally. It can be concluded that the definition of the concept of crime Technology or Cyber crime is a criminal act that is committed using technological tools, namely computers and utilizing the development of internet technology as the main crime tool.[7]

Cybercrime has characteristics based on the scope of the crime, the nature of the crime, the perpetrators of the crime, the mode of crime, and the type of loss caused. Cybercrime is also classified into three groups, namely:

1. Cybercrime has characteristics based on the scope of the crime, the nature of the crime, the perpetrators of the crime, the mode of crime, and the type of loss caused. Cybercrime is also classified into three groups, namely: Cybertresspass Cybertresspass refers to the act of entering or accessing a computer system, network, or data without permission from its owner. This can include a variety of activities, such as hacking, where individuals or groups gain illegal access to steal information, damage data, or commit other malicious acts. Cybertresspass is often considered a violation of the law, as it violates the privacy and security rights of the system owner. Law enforcement in many countries has introduced strict regulations to counter this behavior.[8]
2. Cybervandalism is the act of damaging or altering information on a website or computer system with malicious intent. This can include defacing a website, where the site's appearance or content is altered unlawfully, or attacking the system with viruses or malware. Cybervandalism is often done to demonstrate protests, convey political messages, or just for entertainment. These actions not only harm the site

[6] Lita Sari Marita, "Cybercrime and the Application of Cyberlaw in the Eradication of Cyberlaw in Indonesia," no. 18 (2020): 6.

[7] Lita Sari Marita, "Cybercrime and the Application of Cyberlaw in the Eradication of Cyberlaw in Indonesia," no. 18 (2020): 6.

[8] Eliasta Ketaren, "Cybercrime, Cyber Space, and Cyber Law" V, no. 2 (2016): 35–42.

owner but also interfere with the experience of other users and can cause significant financial or reputational losses.

Types of Cybercrime include the following:

a. Cyberterrorism
A cybercrime is included in the category of cyber terrorism if it threatens many people, namely the government or citizens, one of which is the act of cracking to government or military websites. The National Police Agency of Japan (NPA) defines cyber terrorism as electronic attacks through computer networkings againstcritical infrastructures that have potential critical effects and economic activities of that nation.[9] So this cyberterrorism attacks the government and makes the government an object with a scary motive to scare the public by terrorizing, hijacking or threatening security and disrupting the government system.

b. Cyber-pornography
Cyber-pornography refers to the dissemination and consumption of pornographic content through digital media, including the internet, applications, and video-sharing platforms. This phenomenon includes different types of sexually explicit material, which can be easily accessed by users all over the world. Although cyber-pornography is often considered a form of sexual expression, there are a variety of issues that arise related to social, mental health, and ethical impacts, especially regarding its accessibility for children and adolescents. In addition, many countries have regulations regulating the spread of pornographic content, including laws that prohibit child pornography and regulate oversight of adult content. Cyber-pornography cases also involve considerations about privacy rights, consent, and potential exploitation that can occur in the production and distribution of such content.

c. Cyber-harrassment
Cyber-harassment is a form of harassment that is carried out online, in which an individual or group uses information technology, such as social media, email, or messaging apps, to intimidate, threaten, or harass others. These actions can include sending offensive messages, spreading rumors or false information, and repeated harassment that causes victims to feel depressed or threatened. Cyber-harassment can have a serious impact on the victim's mental and emotional health, often leading to stress, anxiety, and depression. In many countries, cyber-harassment is considered a violation of the law, and there are efforts to raise public awareness of the issue and provide support for victims.

d. Cyber-stalking crimes of stalking
Cyber-stalking is a form of online bullying, in which a person repeatedly supervises, intimidates, or threatens another individual using information and communication technology. These actions can include sending intrusive messages, tracking location through social media, or disseminating personal information without permission. Cyber-stalking often causes fear and anxiety in victims, and can have a serious impact on their mental and emotional health. In many cases, cyber-stalking can progress to more aggressive physical behavior, making it a serious problem that requires legal attention.

e. Hacking and Cracker

[9] Lita Sari Marita, "Cybercrime and the Application of Cyberlaw in the Eradication of Cyberlaw in Indonesia."

A hacker is someone who has an interest in learning computer systems in deep detail and has a talent for improving capabilities. Then some of these hackers often carry out acts of internet destruction commonly called crackers. So a cracker is a hacker who uses his knowledge and abilities for negative things.[10]

f. Carding (credit card fraud)
Carding, or credit card fraud, is an illegal practice in which stolen credit card information is used to make transactions without the owner's permission. This process typically involves stealing credit card data through various methods, such as phishing, hacking, or purchasing data from the black market. After obtaining information, the perpetrator can use the data to purchase goods or services online, or even sell the stolen information to other parties. Carding is a serious crime that can result in significant financial losses for individuals and financial institutions. To combat carding, many financial institutions and technology companies are implementing stricter security measures, such as two-factor authentication and monitoring of suspicious transactions.[11]

g. Cyberquatting and Typosquatting
Cybersquatting and typosquatting is a crime by registering the domain name of another company's name and then trying to sell it to another company at a higher price. The oni crime also makes a plagiarism domain by making it as similar as possible to someone else's domain name, which belongs to the Company's rival domain.[12]

h. Hijacking
Hijacking in the context of the cyber world refers to the act of taking control of a computer system, network, or online account without the owner's permission. This can include different types of attacks. Hijacking can have serious impacts, including personal data theft, financial losses, and privacy breaches. To address these threats, it's important to implement strong security measures, such as the use of two-factor authentication and updated antivirus software.

i. Sabotage and Extortion
Crime intentionally creates a disruption, destruction, destruction of data, computer programs and computer networks. This crime is usually committed by inserting a logic bomb, a computer virus and causing the data to be exposed to a virus so that it is damaged and cannot be opened.

j. Cyber Espionage
It is a crime to spy by using the internet network by entering the computer network system belonging to the party intended to be spied on.[13]

k. Data Forgery
Data forgery is a crime by falsifying data in important documents that exist on the internet and web databases.

Cybercrime based on the motive and purpose of committing the crime is divided into three, namely, Cybercrime that attacks individuals/Against Person, Cybercrime that attacks

[10] Barda Nawawi Arief, The Crime of Mayantara (Jakarta: Rajawali Pers, 2006)

[11] Sastya Hendri Wibowo et al., Cyber Crime in the Digital Era, 2023, https://www.google.co.id/books?id=xOqmEAAAQBAJ.

[12] Sriwulan, "Juridical Review of Cyber Crime in Indonesia" (2023): 1–146, http://repository.iainpalopo.ac.id/id/eprint/7312/1/Skripsi_Sriwulan BUNDELL %283%29.pdf.

[13] Budi Sahariyanto, Information Technology Crime (Cyber Crime) Urgent Regulation and Legal Loopholes (Jakarta: Rajawali Press, 2012).

property rights/Againts Property, and Cybercrime that attacks the government/Againts Government. Then it is observed from the type of cybercrime activity that there are two mentions that cybercrime is considered a purely criminal act, when this crime is committed against the background of the motive of the criminal act. For example, carding by doing it with the intention of stealing or taking someone else's credit card number. There is also the assumption that cybercrime is a gray crime, meaning that in this form of crime it must be difficult to determine and difficult to categorize whether what is done is included in a criminal act or not, this is because the motive used in committing this crime is still new and has never been used before in this crime.[14]

The Implementation of Cyberlaw in Indonesia

The implementation of Cyberlaw in Indonesia involves various regulations and policies aimed at regulating activities in cyberspace, protecting users' rights, and preventing cybercrime. The implementation of Cyberlaw in Indonesia is becoming increasingly important along with the rapid development of information and communication technology. With the increasing use of the internet in various aspects of life, both personal and business, the need for regulations that regulate activities in cyberspace is increasingly urgent. Cyberlaw in Indonesia encompasses a wide range of laws and policies that aim to protect users, prevent cybercrime, and ensure information security. One of the main foundations of Cyberlaw in Indonesia is the Electronic Information and Transaction Law (ITE Law) which was passed in 2008. This law regulates various aspects of electronic transactions, including regulations on the organization of electronic information, the responsibilities of service providers, as well as sanctions for violations, such as fraud and defamation. With the ITE Law, people are expected to be able to transact more safely and responsibly in cyberspace.

In addition, Indonesia has also passed the Personal Data Protection Law (PDP Law) in 2022. The Act aims to protect individuals' personal data from misuse and give individuals control over their data. This regulation is very important considering the large amount of data obtained and processed by companies and government agencies. With the PDP Law, it is hoped that there will be an increase in awareness of the importance of personal data protection among the public and companies. The Government of Indonesia, through the State Cyber and Cryptography Agency (BSSN), is also active in developing cybersecurity policies. BSSN is tasked with protecting the country's critical infrastructure as well as handling cyber incidents. International cooperation is also one of the focuses, where Indonesia participates in various forums and agreements to combat cybercrime globally. This effort demonstrates Indonesia's commitment to creating a safe and trusted digital environment.[15]

Cyberlaw is a law that regulates the use of internet networks or activities in cyberspace. The scope of cyberlaw in Indonesia is Public Law and Private Law. Public law consists of jurisdiction, ethics of online activities, consumer protection, anti-monopoly, taxation, fair competition, regulatory body, data protection, and cybercrimes. Meanwhile, in private law, it consists of IPR, E-Commerce, Cyber Contract, Domain Name, Insurance. Cyber Law is very important because today's internet-based activities are not bound by the country's territorial boundaries and can be done at any time. Although the evidence used is

[14] Tanbela Zein Vitadiar et al., Ethics and Cyber Law (Magetan: CV. AE Mqedia Graphics, 2021), pp. 85-87.

[15] Faizur Rashid and Sadaf Rashid, "Cyber Laws," *Digital Freedom* (2023): 85–133.

virtual and electronic, cyber activity is an activity that has a real impact. To deal with the threat and adverse impact of cybercrime, several international organizations conduct joint research and studies to discuss cybercrime. As a result of the cooperation of international organizations, international law on cybercrime was formed.[16]

The first international organization was called the Organisation for Economic Co-Operation and Development (OECD) which was first formed and fought cybercrime cases in 1983 and 1985. The second organization is the United Nations (UN) in collaboration with the United Nations (UN), the third organization, The Group Of Eight (G8) which contains industrial countries. The fourth organization was the Council of Europe (CoE) in 2001. Meanwhile, in Indonesia itself, from the discussion of the House of Representatives meeting on March 25, 2008 which approved the ITE Bill, it was then stipulated into law and on April 21, 2008 by the President of the Republic of Indonesia it was promulgated as Law No. 11 of 2008 concerning Information and Electronic Transactions Statute Book of 2008 No. 58. The Electronic Information and Transaction Law (Undang-Undang ITE) is the first cyber law in Indonesia that was established to provide legal certainty for people who conduct electronic transactions.[17]

The goal is to encourage economic growth, prevent information and communication technology-based crimes, and protect the people who use these technology services. The ITE Law consists of 54 articles organized into 13 chapters. The content and explanation of Law No. 11 of 2008 concerning Electronic Information and Transactions and Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions, are as follows:

1. Acts of Violating Morality, contained in article 27 paragraph (1) of Law Number 11 of 2008, which reads "Every Person deliberately and without the right to share or disseminate or make accessible Electronic Information or Electronic Documents that have content that violates morality".
2. Gambling, Online gambling is regulated in Article 27 paragraph (2) of the Electronic Information and Transaction Law. The regulation also states that: "Any person who knowingly and without rights shares, disseminates, or creates electronic information or electronic documents containing elements of gambling may be subject to sanctions."
3. Insult or defamation, this act is regulated in Article 27 Paragraph (3) of the Law on Information and Electronic Transactions. which reads: "Every person intentionally, and without the right to share/disseminate/make accessible electronic information/electronic documents that have insulting or defamatory content." Lawmakers identify insults and defamation as equivalents. Insult is an act, while desecration is a form of insult. Apparently, the lawmakers want to direct the acts of insult that occur in the internet media as a form of pollution. Acts of insult and defamation often appear in various comment columns on the internet, especially when victims are identified through their personal identities, photos, or videos. Perpetrators can write derogatory or defamatory comments on public walls to convey statements or associate those statements with the victim.
4. Extortion or threats, contained in article 27 paragraph (4) of Law No. 11 of 2008. And in article 368 (1) of the Criminal Code, the acts of extortion and threats are more clearly classified

[16] Ahmad Ramli, Cyber Law and IPR in the Indonesian Legal System (Bandung: Refika Aditama, 2010), p. 2.

[17] Sigid Suseno, Jurisdiction of Cyber Crime (Bandung: Refika Aditama, 2012), p. 125.

5. Cyberstalking, the explanation of which is stated in Law No. 11 of 2008 Article 29. The provisions regarding information and electronic transactions in Article 29 regulate acts of harassment, threats, or other actions taken to cause fear, including certain words or actions.
6. The spread of fake news (hoax) is regulated in Law No. 11/2008 Article 28 Paragraph 1.
7. Hate Speech is contained in article 28 paragraph (2) of Law No. 11/2008 Illegal Access, Regulated in Law No. 11 of 2008 article 30.[18]

The principles of Cyberlaw cover the basic principles that are the foundation of legal regulation in the digital world. Here are some of the principles that are commonly applied in Cyberlaw.

1. Subjective Territoriality, in this perspective, the law applies based on the scene of cybercrime.
2. Objective Territoriality, Law applies based on where the main consequences of the crime occur.
3. Nationality, in this perspective, the state has the jurisdiction to determine the law based on the nationality of the perpetrator.
4. Passive Nationality, which focuses jurisdiction based on the nationality of the victim.
5. In this perspective, the law is based on the desire of the state to protect its interests from crimes that occur outside its territory, especially when the victim is the state or the government itself.
6. Universality, This principle should receive special attention in the legal handling of cyber cases. Also known as "universal interest jurisdiction," this principle essentially stipulates that every country has the right to arrest and punish perpetrators of piracy.[19]

Implications of the Role of Stakeholders in the Implementation of Cyberlaw

Stakeholders in the context of the implementation of Cyberlaw consist of various parties who have interests and roles in the digital ecosystem.[20] The role of stakeholders in the implementation of Cyberlaw is crucial to create a safe and orderly digital ecosystem. Stakeholders include a wide range of stakeholders, including governments, law enforcement agencies, the private sector, communities, non-governmental organizations (NGOs), academics, and the media. Each party has different responsibilities and contributions, which complement each other in efforts to enforce cyber laws and protect users in cyberspace.

a. Government and Law Enforcement Agencies
The government has the main responsibility in formulating and implementing regulations that regulate activities in cyberspace. This includes the development of laws, cybersecurity policies, and law enforcement against Cyberlaw violations. In addition, the government is also tasked with providing education to the public about their rights and responsibilities in the digital world. Law enforcement agencies, such as the police,

[18] Miftakhur Rokhman Habibi and Isnatul Liviani, "Information Technology Crime and Its Countermeasures in the Indonesian Legal System," Al-Qanun: Journal of Islamic Law Thought and Reform 23, no. 2 (2020): 400–426.

[19] Rashid and Rashid, "Cyber Laws."

[20] M. Syukri Akub, "Regulation of Cyber Crime in the Indonesian Legal System" 3, no. 2 (2018): 91–102.

play a role in investigating and following up on cybercrime cases. They also collaborate with international institutions to deal with crimes of a cross-border nature. Special training to handle Cyberlaw cases is also important for law enforcement officials to be able to perform their duties effectively.

b. Private Sector and Community
Technology companies and internet service providers have a responsibility to comply with Cyberlaw regulations and implement adequate security measures. They also play a role in protecting user data and preventing misuse of information. In addition, the private sector can contribute to education and training regarding cybersecurity for employees and customers. And the community as information technology users has an important role in the implementation of Cyberlaw. Awareness of digital rights, security, and online ethics is indispensable for users to protect themselves from cybercrime. Education on how to report violations and understand existing regulations is also important to increase public participation in maintaining the digital environment.

c. Non-Governmental Organizations
Non-governmental organizations that focus on human rights, privacy, and cybersecurity issues can provide a voice for the public in the development of Cyberlaw regulations. They play a role in advocating for the protection of digital rights and raising awareness about issues related to cybercrime and its impact on individuals and communities.[21]

d. Academics and Researchers
Academics and researchers contribute to the development of Cyberlaw through in-depth studies and analyses of cybercrime trends, their impacts, and the effectiveness of existing regulations. This research can help governments and related institutions in formulating better policies and responding to challenges in the digital world.

e. Media and Legal Practitioners
The role of the media in disseminating information about Cyberlaw and raising public awareness about cybersecurity issues. And the role of a lawyer or legal practitioner Legal professionals who focus on Cyberlaw-related issues and provide legal advice to individuals and organizations

CONCLUSION

The development of information and communication technology in the era of globalization has had a significant impact on the lives of the Indonesian people, with the number of internet users reaching more than 200 million people by 2023. Although it provides various conveniences, technology also brings challenges in the form of cybercrime which comes in various forms such as cyberpiracy, cybertrespass, and cybervandalism. In response to this threat, Indonesia has developed a cyber legal framework (cyberlaw) through ITE Law No. 11 of 2008 and the PDP Law of 2022. The implementation of cyberlaw in Indonesia is based on six fundamental legal principles and involves a wide range of stakeholders. The role of stakeholders in the implementation of cyberlaw is very important, where the government and law enforcement agencies play a role in formulating and implementing regulations, the private sector is responsible for data security and protection, non-governmental organizations advocate for the protection of digital rights, academics contribute to research and development, and the media play a role in cybersecurity socialization.

[21] Zahra Anisa Wira Yuda, Hastuti Rahmasari, and Tri Agus Gunawan, "The Effectiveness and Application of Criminal Law to Cybercrime in Indonesia," Causa: Journal of Law and Citizenship 4, no. 10 (2024): 61–70.

REFERENCES

Ahmad Ramli. Cyber Law and IPR in the Indonesian Legal System. Bandung: Refika Aditama, 2010.

Barda Nawawi Arief. Mayantara Crime. Jakarta: Rajawali Press, 2006

Budi Sahariyanto. Information Technology Crime (Cyber Crime), the Urgency of Regulation and Legal Loopholes. Jakarta: Rajawali Press, 2012

Eliasta Ketaren. "Cybercrime, Cyberspace, and Cyber Law" V, no. 2 (2016): 35–42

Habibi, Miftakhur Rokhman, and Isnatul Liviani. "Information Technology Crime (Cyber Crime) and Its Countermeasures in the Indonesian Legal System." Al-Qanun: Journal of Islamic Law Thought and Reform 23, no. 2 (2020): 400–426

Hengki Irawan et al. "Regulation of Cyber Crime in the Indonesian Legal System." Journal Of Social Science Research Volume 4, no. 1 (2024): 4358–4369

Lita Sari Marita. "Cybercrime and the Application of Cyberlaw in the Eradication of Cyberlaw in Indonesia," no. 18 (2020): 6.

M. Syukri Akub. "Regulation of Cyber Crime in the Indonesian Legal System" 3, no. 2 (2018): 91–102

Markus Djarawula, Novita Alfiani, and Hanita Mayasari. "Juridical Review of Information Technology Crimes (Cybercrime) in Indonesia is reviewed from the perspective of Law Number 11 of 2008 concerning Information and Electronic Transactions." Journal of Scientific Horizons 2, no. 10 (2023): 3799–3806

Risky Rilandi refused. "Juridical Review of Cyber Crime Based on Criminal Law." Journal of Law and Socio-Politics Vol 1 No. (2023)

Rashid, Faizur, and Sadaf Rashid. "Cyber Laws." Digital Freedom (2023): 85–133

Riko Nugraha. "Indonesian Legal Perspective (Cyberlaw) Handling Cyber Cases in Indonesia." Scientific Journal of Aerospace Law Vol 11 No. (2021)

Sigid Suseno. Cybercrime Jurisdiction. New York: Refika Aditama, 2012

Sriwulan. "Juridical Review of Cyber Crime in Indonesia" (2023): 1–146. http://repository.iainpalopo.ac.id/id/eprint/7312/1/Skripsi_Sriwulan BUNDLE %283%29.pdf

Vitadiar, Tanbela Zein, Ginanjar Setyo Permadi, Rocky Ardiansyah Yudistira Putra, and Unzilla Savika Putri. Cyber Ethics and Law. Magetan: CV. AE Mqedia Graphics, 2021

Wibowo, Sastya Hendri, Joseph Dedy Irawan, Wahyuddin S, Bambang Winardi, Leo Willyanto Santoso, Safrizal, Yuniansyah, et al. Cyber Crime in the Digital Era, 2023. https://www.google.co.id/books?id=xOqmEAAAQBAJ

Yuda, Zahra Anisa Wira, Hastuti Rahmasari, and Tri Agus Gunawan. "Effectiveness and Application of Criminal Law on Cybercrime in Indonesia." Causa: Journal of Law and Citizenship 4, no. 10 (2024): 61–70.

"Cybercrime - Indonesian Wikipedia, the free encyclopedia." Accessed October 23, 2024. https://id.wikipedia.org/wiki/Kejahatan_siber.