International Journal of Health, Economics, and Social Sciences (IJHESS)
Vol. 6, No. 4, October 2024, pp. 1156~1159
DOI: 10.56338/ijhess.v6i4.6269
Website: https://jurnal.unismuhpalu.ac.id/index.php/IJHESS

The Role of Criminal Law in Handling Cyber Crimes: Challenges and Solutions

Maria Alberta Liza Quintarti[1*], Riadi Asra Rahmad[2], Zulkarnain S[3], Budi Handayani[4], Rica Gusmarani[5]
[1]Universitas Flores
[2]Universitas Islam Riau
[3]Universitas Islam Riau
[4]Universitas Sunan Giri Surabaya
[5]Universitas Deli Sumatera

Article Info

Article history:

Received 22 September, 2024
Revised 24 October, 2024
Accepted 24 October, 2024

Keywords:

Criminal Law;
Cyber Crime;
Challenges;
Solutions

ABSTRACT

Cybercrime includes various illegal acts committed via the internet or digital technology. With the rapid development of information technology, criminal law is faced with new challenges in dealing with this crime. Cybercrime is any unlawful act carried out via a computer, network or digital device that can harm individuals or society as a whole. Among the forms of cybercrime are online fraud, identity theft, malware and ransomware, hacking and also cyberbullying. In this crime, criminal law has a vital role in dealing with cybercrime through law enforcement, crime prevention, victim protection, increasing law enforcement capabilities, and international cooperation. Continuous efforts are needed to ensure the law can keep up with technological developments and the changing dynamics of crime. Even though it also faces various challenges, it can take appropriate solution steps, such as strengthening regulations, international cooperation, and increasing awareness, so that it can be more effective in fighting cybercrime and protecting society in general.

Corresponding Author:

Maria Alberta Liza Quintarti
Universitas Flores
Email: lizaquintarti36@gmail.com

INTRODUCTION

Cybercrime, or cybercrime, is an illegal act carried out using computer technology and internet networks. According to Brian D. McCarthy, he also explained that cybercrime includes various types of crimes that can occur in cyberspace, including fraud, data theft and the spread of malware. (McCarthy, B. D. 2021).

Kumar also explained that Cybercrime is any unlawful act carried out via a computer, network or digital device that can harm individuals or society as a whole. (Kumar, 2022) This crime can be committed by individuals, groups, or even structured organizations, and the impact can be very broad, ranging from financial loss to reputational damage.

Cybercrime, which includes all forms of criminal activity carried out via computer networks and the internet, has grown rapidly along with advances in technology. Criminal law has a crucial role in overcoming this problem, but faces various complex challenges.

Several expert views explain the role of criminal law, namely as follows:

Hans Kelsen, Kelsen believes that criminal law functions to protect society from detrimental actions, by providing sanctions against violators. Criminal law aims not only to punish, but also to prevent crime.

Bernard Harcourt, in his view, Harcourt emphasizes that criminal law has a role in creating social order. Criminal law helps maintain justice and provides a sense of security for society.

Emile Durkheim, durkheim saw criminal law as a reflection of the values and norms that apply in society. He believes that criminal law functions to strengthen social solidarity and create collective awareness.

Franz von Liszt, liszt argued that criminal law must function not only as a punitive tool, but also as a rehabilitative tool. Criminal law must pay attention to the aspect of coaching for offenders to reduce the possibility of crime recurring.

David Garland, garland argues that criminal law also plays a role in creating social narratives about crime. Through law enforcement, society develops an understanding of what is considered deviant behavior and how to deal with it.

So this research will discuss the Role of Criminal Law in Handling Cyber Crime which includes a discussion of the challenges and also the solutions.

METHODOLOGY

Methodology essentially provides guidelines on how to study, analyze and understand the object being researched. Methodology is an element that is absolutely present in research (Soekanto, 2014). The research method used by this journal article to discuss the problems that have been determined is using normative research methods. Normative Legal Research is legal research carried out by examining library materials or secondary data (Soekanto & Mamudji, 2003). According to Peter Mahmud Marzuki, normative legal research is a process of finding legal rules, legal principles and doctrines in law in order to answer the legal issues faced (Marzuki, 2010). In this type of legal research, law is often conceptualized as what is written in statutory regulations or law is conceptualized as rules or norms which are benchmarks for human behavior that is considered appropriate (Amiruddin & Asikin, 2006).

In this research, the author uses a normative juridical legal research approach, namely research that focuses on examining the application of rules or norms in positive law, namely statutory regulations, legal theories related to the problems to be discussed. According to Johnny Ibrahim, there are 7 (seven) approaches in normative legal research, namely: "Statutory approach), conceptual approach, analytical approach, comparative approach, historical approach. approach), philosophical approach, and case approach".

The research specification in this research is analytical descriptive research. Descriptive means that in this research the author intends to describe and explain in detail, systematically and comprehensively everything related to legal aspects that need to be considered in relation to the problem to be studied.

RESULTS AND DISCUSSION

The Role of Criminal Law in Handling Cyber Crime

Cybercrime includes various illegal acts committed via the internet or digital technology. With the rapid development of information technology, criminal law is faced with new challenges in dealing with this crime. Cybercrime is any unlawful act carried out via a computer, network or digital device that can harm individuals or society as a whole. (Kumar, 2022)

There are several types or forms of cybercrime that often occur, namely as follows:

Online Fraud

Online Fraud includes fraudulent schemes such as phishing, where criminals try to obtain personal information through fake emails or websites. Jim Geovedi states that online fraud is one of the most common forms of crime, with many victims unaware that they have been conned. (Geovedi, J. 2023).

Identity Theft

Identity theft occurs when someone uses another person's personal information to gain access to an account or conduct illegal transactions. Laura L. K. Baker notes that identity theft can damage a victim's reputation and cause significant financial loss. (Baker, L. L. K. 2020).

Malware and Ransomware

Malware is malicious software that is used to damage or access a system without permission. Ransomware, on the other hand, encrypts the victim's data and demands a ransom to return it. Michael J. Smith mentioned that ransomware attacks have increased in recent years, targeting both individuals and large organizations. (Smith, M. J. 2023).

Hacking

Hacking is the act of entering a computer system or network without permission to steal data, destroy information, or spread viruses. According to Kevin Mitnick, a former hacker, many hacking actions are driven by the desire to prove technical abilities, even though the impact can be detrimental to many parties. (Mitnick, K. 2022).

Cyberbullying

Cyberbullying involves using the internet or digital devices to intimidate or harass individuals, often through social media. Holly D. Johnson emphasizes that cyberbullying can have a serious impact on the victim's mental and emotional health, including the risk of depression and anxiety. (Johnson, H. D. 2021).

Criminal law has an important role in dealing with increasingly complex and detrimental cyber crimes. This crime includes various illegal acts carried out via computer networks and the internet. Therefore, appropriate regulations and effective law enforcement are very necessary to protect the public. Among the roles of criminal law in dealing with cybercrime are as follows:

Upholding Law and Justice

Criminal law functions to uphold justice by providing sanctions to perpetrators of cybercrime. Kumar stated that the presence of criminal law creates legal certainty and provides a sense of security for society. (Kumar, M. A. K. G. S. S. 2022).

Prevent Crime

Sanctions stipulated in criminal law also function as a deterrent effect, namely to prevent individuals from committing crimes. James D. Watson argues that the deterrent effect of criminal law can reduce the number of cybercrimes. (Watson, J. D. 2021).

Protecting Victims

Criminal law provides protection and justice for crime victims. With clear legal provisions, victims can file claims and obtain compensation. Laura L. K. Baker emphasizes the importance of legal protection for cybercrime victims to restore their rights. (Baker, L. L. K. 2020).

Increasing Law Enforcement Capacity

Criminal law also plays a role in providing a framework for law enforcement to handle cybercrime cases. Michael J. Smith notes that adequate training and resources are necessary for law enforcement officials to conduct effective investigations of these crimes. (Smith, M. J. 2023).

International Cooperation

Because many cybercrimes are transnational in nature, criminal law plays an important role in building international cooperation. Markus T. Fisher stated that international agreements and cooperation between countries are needed to combat this crime effectively. (Fisher, M. T. 2023).

Criminal Law Challenges in Handling Cyber Crime and Their Solutions Among the challenges of criminal law in dealing with cybercrime are as follows:

Characteristics of Crime

Cybercrime is often transnational in nature, which complicates the legal process due to differences in regulations in each country. (Barlow, J. 2021).

Anonymity

Perpetrators can operate anonymously, making it difficult to identify and catch them. (Smith, R. 2022).

Rapid Technological Development

Laws often lag behind new technological developments, making it difficult to formulate effective regulations. (Jones, A. 2023).

Lack of Public Awareness

The public and law enforcement often lack understanding of the forms and impacts of cybercrime, hampering prevention and law enforcement efforts. (Williams, T. 2020).

Of these challenges, there are several solutions that can be used as concrete steps to overcome these challenges, including the following:

Strengthening Regulations

Update laws governing cybercrime to suit current technological developments. Some countries have begun adapting their regulations to better cover cybercrime. (Lee, C. 2019).

International Cooperation

Building cooperation between countries in law enforcement, including extradition treaties and information exchange. (Brown, M. 2020).

Education and Awareness

Conduct educational campaigns to increase public awareness about the risks of cybercrime and how to protect themselves from these threats. (Patel, S. 2021).

Training for Law Enforcement

Provide special training for law enforcement officers on investigative techniques and technology related to cybercrime, so that they are better prepared to handle these cases. (Adams, J. 2022).

CONCLUSION

So it can be concluded that criminal law has a vital role in dealing with cybercrime through law enforcement, crime prevention, victim protection, increasing law enforcement capabilities, and international cooperation. Continuous efforts are needed to ensure the law can keep up with technological developments and the changing dynamics of crime. Even though it also faces various challenges, it can take appropriate solution steps, such as strengthening regulations, international cooperation, and increasing awareness, so that it can be more effective in fighting cybercrime and protecting society in general.

SUGGESTION

Lawyers must always adapt to this technological era in dealing with cybercrime and carry out more complete legal measures that can provide solutions in handling cybercrime.

REFERENCES

Adams, J. (2022). "Training Law Enforcement for Cybercrime Investigations: Best Practices." Law Enforcement Technology Journal, 15 (3).

Amiruddin, & Asikin, Zaenal. (2006). Pengantar Metode Penelitian Hukum. Jakarta: PT. Raja Grafindo Persada.

Baker, L. L. K. (2020). "Identity Theft in the Digital Age: Risks and Prevention." Journal of Cyber Law, 5 (4).

Barlow, J. (2021). "International Cooperation in Cybercrime: Challenges and Solutions." Cybersecurity Journal, 34 (2).

Brown, M. (2020). "The Role of International Treaties in Combatting Cybercrime." Global Cybersecurity Review, 9 (1).

Fisher, M. T. (2023). "International Cooperation in Cybercrime Enforcement." Journal of Global Cybersecurity, 11 (2).

Geovedi, J. (2023). "Online Fraud: A Growing Threat." Cybercrime Review, 12 (3).

Johnson, H. D. (2021). "Cyberbullying: Impacts on Mental Health." Journal of Adolescent Health, 58 (6).

Jones, A. (2023). "Adapting Legal Frameworks to Technological Advances: The Case of Cybercrime." Technology and Law Review, 12 (3).

Kumar, M. A. K. G. S. S. (2022). "Understanding Cybercrime: Definitions and Concepts." International Journal of Cybersecurity, 8 (1).

Lee, C. (2019). "Legislating Cybercrime: Recent Developments and Future Directions." International Journal of Cyber Law, 7 (2).

Marzuki, P. (2010). Penelitian Hukum. Jakarta: Kencana Prenada.

McCarthy, B. D. (2021). "The Rise of Cybercrime: A Global Perspective." Journal of Digital Security, 15 (2).

Mitnick, K. (2022). "Hacking: The Art of Exploitation." Cybersecurity Today, 10 (2).

Patel, S. (2021). "Enhancing Public Awareness of Cyber Threats: A Community Approach." Cyber Safety Journal, 22 (5).

Smith, M. J. (2023). "Malware and Ransomware: Understanding the Threat Landscape." Global Cybersecurity Review, 19 (1).

Smith, R. (2022). "The Anonymity Dilemma: Addressing Challenges in Cybercrime Investigation." Journal of Digital Law, 45 (1).

Soekanto, S. (2014). Pengantar Penelitian Hukum. Jakarta: Universitas Indonesia Press.

Soekanto, S., & Mamudji, S. (2003). Penelitian Hukum Normatif : Suatu Tinjauan Singkat. Jakarta: PT. Raja Grafindo Persada.

Watson, J. D. (2021). "The Deterrent Effect of Criminal Law on Cybercrime." Journal of Cyber Law & Policy, 14 (3).

Williams, T. (2020). "Public Awareness and Education on Cybercrime: A Necessity for Effective Prevention." Journal of Cybersecurity Education, 18 (4).