JURNAL MULTIDISIPLIN MADANI (MUDIMA)

Homepage: https://journal.formosapublisher.org/index.php/mudima
ISSN: 2808-5639 (Online)
Research Article

Volume 4, No 1, January (2024)	DOI: https://doi.org/10.55927/mudima.v4i1.7962	Page: 168-173

Evolution of Cybercrime Law in Legal Development in the Digital World

Isra Ruddin[1]*, Subhan Zein SGN[2]

[1]Dosen LSPR Institute of Communications & Business

[2]Dosen Universitas Dirgantara Marsekal Suryadarma

Corresponding Author: Isra Ruddin israruddin@lspr.edu

ARTICLE INFO

Keywords: Cybercrime Law, Information and Communication Technology, Cross-Border Cooperation, Data Protection, Law Enforcement, Cybercrime Threats

Received : *2 November*
Revised : *20 December*
Accepted : *9 January*

ABSTRACT

This research explores the evolution of cybercrime law in the face of developments in information and communication technology (ICT) over the last few decades. The development of digital technology has provided countless benefits but has also given rise to increasingly complex threats in the form of cyber attacks and cybercrime. This research aims to investigate how cybercrime law has evolved in response to changes in ICT and how these developments have influenced the effectiveness of cybercrime law enforcement. This research also analyzes the role of cross-border cooperation in cybercrime law enforcement and how developments in international law have influenced countries' ability to deal with global cybercrime threats. The research results show that the evolution of cybercrime law includes the establishment of more specific cybercrime laws and stronger protection of personal data. Cross-border cooperation plays an important role in cybercrime law enforcement, including information exchange, joint prosecution, asset freezing, and extradition. Developments in international law, such as the Budapest Convention and the General Data Protection Regulation (GDPR), have provided the legal basis necessary for more effective cross-border cooperation. However, challenges remain, including legal and jurisdictional differences between countries that often hamper law enforcement efforts. Therefore, increasing international cooperation and efforts to overcome these obstacles is critical in maintaining security and privacy in the ever-evolving digital era

INTRODUCTION

The digital world has experienced rapid development over the last few decades. The information and communications technology (ICT) revolution has shaped the way we communicate, work, shop and even play. Meanwhile, the countless advantages and innovations offered by digital technology also bring serious challenges in the form of cybercrime better known as cybercrime. Crimes such as data theft, hacking, online fraud, the spread of malware, and privacy violations have become increasingly troubling threats.

This very rapid development has forced legal systems around the world to adapt to new needs in protecting society from increasingly sophisticated cybercrime threats. Therefore, studies regarding the evolution of cybercrime law in the development of law in the digital world are very relevant and important.

Initially, laws relating to cybercrime tended to be limited and inadequate. Existing laws often cannot address crimes that exploit the special characteristics of digital technology, such as anonymity and global coverage. Therefore, cybercrime law was first presented as a response to technological developments.

The evolution of cybercrime law includes various aspects that must be understood. One of these is a change in the legal approach to cybercrime. Initially, laws tended to focus on more conventional law enforcement. However, as the frequency and complexity of cyber-attacks increase, the law is adapting to provide stronger tools and authority for law enforcement and cybersecurity policy. In addition, the protection of individual rights and privacy is also a key issue in the evolution of cybercrime law. To protect citizens from unauthorized dissemination of personal data and misuse of personal information, laws have evolved to create stronger data protection frameworks. This includes data protection laws, rules on disclosing data breaches, and data management guidelines.

Another relevant development in the evolution of cybercrime law is cross-border cooperation. Cybercrime often crosses countries and jurisdictions. Therefore, there is a need for international cooperation in dealing with these crimes. Several international agreements and conventions have been created to facilitate cooperation between countries in enforcing cybercrime laws.

While the law continues to evolve to address cybercrime, the challenges facing cybercrime law never end. Increasingly complex cyber-attacks and constant changes in technology force the law to remain up-to-date and relevant. Therefore, in-depth research on the evolution of cybercrime law in the development of law in the digital world is very important to understand how the law can continue to protect society in this digital era.

METHODS

The evolution of cybercrime law includes the establishment of more specific cybercrime laws and stronger protection of personal data. Cross-border cooperation plays an important role in cybercrime law enforcement, including information exchange, joint prosecution, asset freezing, and extradition. Developments in international law, such as the Budapest Convention and the General Data Protection Regulation (GDPR), have provided the legal basis necessary for more effective cross-border cooperation.

RESULTS AND DISCUSSION

Development of Cybercrime Law in Response to Developments in Information Technology Over the past few decades, developments in information and communications technology (ICT) have significantly changed the legal landscape of cybercrime. The historical evolution of the law in response to these developments reflects marked changes in cybercrime legal acts, regulations, and law enforcement approaches. The biggest challenge faced is how the law can continue to maintain its relevance in the face of increasingly complex cyber-attacks. The main question is to what extent these legal developments have affected the effectiveness of cybercrime law enforcement.

At the beginning of the digital era, cybercrime laws tended to be limited and unable to deal with increasingly clever cyber attacks. Classical laws that focus on conventional crime are often incapable of investigating or prosecuting cybercrime perpetrators. In response, legislators and policymakers around the world are beginning to review their legal frameworks.

One of the most significant changes is the establishment of more specific cybercrime laws. This law is designed to tackle cybercrime by giving more authority to law enforcement. They cover a wide range of criminal acts such as hacking, data theft, online fraud and the spread of malware. Over time, such laws have been adopted in many countries, providing law enforcement with more effective tools to deal with cyberattacks. Personal data protection law has also undergone important developments. To protect individual privacy, many countries have introduced strict data protection laws. For example, the General Data Protection Regulation (GDPR) in the European Union has become a milestone in the protection of personal data and provides serious consequences for its violations. This creates incentives for companies and entities that process data to be more careful in the management of personal data.

While the law continues to evolve, cybercrime law must also face challenges in carrying out effective law enforcement. Increasingly sophisticated and complex cyberattacks force law enforcement to continually update their skills. The international nature of cybercrime also raises questions about cross-border cooperation and the extradition of cybercrime perpetrators.

Cross-border cooperation is key in enforcing cybercrime law. It involves agreements between countries, exchange of information, and joint efforts in dealing with cyber attacks. However, this cooperation is often complicated by differences in jurisdiction and state regulations. How international law has influenced countries' ability to deal with the global threat of cybercrime is a question that needs to be answered. In conclusion, the evolution of cybercrime law in the development of ICT has resulted in significant changes in the legal framework used to protect society from cyber attacks. Although laws have evolved to address these challenges, cybercrime law enforcement remains a complex and ongoing challenge that requires ongoing efforts to maintain security and privacy in the digital age.

The Role of Cross-Border Cooperation in Cybercrime Law Enforcement Efforts Cross-border cooperation plays a crucial role in efforts to enforce cybercrime law and overcome global cyber threats. In an increasingly interconnected digital era, cyber-attacks are no longer limited to national borders, and international cooperation is a necessity. Developments in international law have influenced countries' ability to deal with global cybercrime threats in various ways.

The role of cross-border cooperation in cybercrime law enforcement is very important because cyber attacks often involve perpetrators from different countries. Investigating these attacks often requires collaboration between law enforcement agencies from various countries, the exchange of information, and complementary legal assistance. Some of the roles of cross-border cooperation in cybercrime law enforcement are:

1. Information Exchange: Countries can share data and information regarding cyber-attacks, perpetrators, or tools used. This allows law enforcement to better understand the perpetrator's tactics.
2. Joint Prosecution: In some cases, cyberattacks involve perpetrators from multiple jurisdictions. Cross-border cooperation allows law enforcement to conduct efficient joint prosecutions.
3. Asset Freezing: International cooperation makes it possible to freeze the assets of perpetrators involved in cybercrime. This can have a major impact on the perpetrator's motivation and prevent further crimes.
4. Extradition: In more serious situations, extradition of the perpetrator to the country concerned can be implemented through existing extradition agreements between countries.

Developments in international law have also provided a legal basis for more effective cross-border cooperation in dealing with global cybercrime threats. Some important developments in international law that impact cybercrime law enforcement include:

1. Budapest Convention on Cybercrime: The Budapest Convention is an international treaty designed to combat cybercrime. It provides a legal basis for cross-border cooperation in the investigation, prosecution and extradition of cybercrime perpetrators.
2. General Data Protection Regulation (GDPR): GDPR is a European Union regulation that regulates the protection of personal data. This affects companies around the world that deal with EU citizens' data and strengthens individual rights in terms of data protection. GDPR requires cross-border cooperation in data protection and handling data breaches.
3. Regional Cooperation: Several regions such as the European Union and ASEAN have developed legal frameworks and regional cooperation mechanisms to face cyber threats together.

However, despite positive developments in international law and cross-border cooperation, there are still several challenges that need to be overcome. Differences in law and jurisdiction between countries often hamper law enforcement efforts. Also, countries lacking adequate capacity and resources may face difficulties in participating in effective cross-border cooperation.

In this increasingly complex context, the role of cross-border cooperation and developments in international law are key in dealing with the global threat of cybercrime. Continuous efforts to improve cooperation and adapt the law to technological developments are essential to maintaining security and stability in an ever-evolving digital world.

CONCLUSION

The evolution of cybercrime law in response to developments in information and communication technology has resulted in significant changes in the legal framework governing cybercrime. These efforts include the establishment of more specific cybercrime laws, stronger personal data protection, and increased cross-border cooperation. However, increasingly clever and complex cyber-attacks are challenging the effectiveness of cybercrime law enforcement.

Cross-border cooperation plays a crucial role in cybercrime law enforcement. Information exchange, joint prosecution, asset freezing and extradition are some of the important aspects of this cooperation. Developments in international law, such as the Budapest Convention and the General Data Protection Regulation (GDPR), have provided the necessary legal foundation for more effective cross-border cooperation.

However, there are still several challenges to overcome. Differences in law and jurisdiction between countries often slow down law enforcement efforts. Countries with limited resources may have difficulty participating in effective cross-border cooperation. Therefore, further efforts in strengthening international cooperation and overcoming these obstacles are essential.

REFERENCES

Alexandrou, A. (2021). Cybercrime and information technology: The computer network infrastructure and computer security, cybersecurity laws, Internet of Things (IoT), and mobile devices. CRC Press.

Alghamdi, M. I. (2020). A descriptive study on the impact of cybercrime and possible measures to curtail its spread worldwide. International Journal of Engineering Research and Technology, 9, 731-5.

Almazkyzy, K., & Esteusizov, Y. N. (2018). The essence and content of cybercrime in modern times. Journal of Advanced Research in Law and Economics, 9(3 (33)), 834-841.

Babanina, V., Tkachenko, I., Matiushenko, O., & Krutevych, M. (2021). Cybercrime: History of formation, current state and ways of counteraction. Amazonia Investiga, 10(38), 113-122.

Belch, G. E., & Belch, M. A. (2018). Advertising and promotion: An integrated marketing communications perspective. mcgraw-hill.

Bunga, D. (2019). Legal response to cybercrime in global and national dimensions. PADJADJARAN Jurnal Ilmu Hukum (Journal of Law), 6(1), 69-89.

Chandler, D., & Fuchs, C. (2019). Digital objects, digital subjects: Interdisciplinary perspectives on capitalism, labour and politics in the age of big data. University of Westminster Press.

Choi, K. S., Lee, C. S., & Louderback, E. R. (2020). Historical evolutions of cybercrime: From computer crime to cybercrime. The Palgrave handbook of international cybercrime and cyberdeviance, 27-43.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2022). Cybercrime and digital forensics: An introduction. Routledge.

Jayasekara, S. D., & Abeysekara, I. (2019). Digital forensics and evolving cyber law: case of BIMSTEC countries. Journal of Money Laundering Control, 22(4), 744-752.

Khan, S., Saleh, T., Dorasamy, M., Khan, N., Tan Swee Leng, O., & Gale Vergara, R. (2022). A systematic literature review on cybercrime legislation. F1000Research, 11, 971.

Kovacs, A. M. (2022). Here there be Dragons: Evolution, Potentials and Mitigation Opportunities of Cybercrime in Nigeria: A Review, Analysis, and Evaluation. Journal of Central and Eastern European African Studies, 2(1).

Losavio, M. M., Pastukov, P., Polyakova, S., Zhang, X., Chow, K. P., Koltay, A., ... & Ortiz, M. E. (2019). The juridical spheres for digital forensics and electronic evidence in the insecure electronic world. Wiley Interdisciplinary Reviews: Forensic Science, 1(5), e1337.

Malik, J. K., & Choudhury, S. (2019). A Brief review on Cyber Crime-Growth and Evolution. Pramana Research Journal, 9(3), 242.

Marion, N. E., & Twede, J. (2020). Cybercrime: An encyclopedia of digital crime. Bloomsbury Publishing USA.

Payne, B. K. (2020). Defining cybercrime. The Palgrave handbook of international cybercrime and cyberdeviance, 3-25.

Rakha, N. A. (2023). Cyber Law: Safeguarding Digital Spaces in Uzbekistan. International Journal of Cyber Law, 1(5).

Ruddin, I. (2023). Manfaat Integrated Marketing Communications dan Penerapan Strategi Content Marketing. Media Sains Indonesia.

Ruddin, I., & Jamalullail, J. (2022). The Development of New Media in the Economic Growth of the Indonesian Music Industry. Ilomata International Journal of Management, 3(4), 470-485.

Ruddin, I., Santoso, H., & Indrajit, R. E. (2022). Digitalisasi Musik Industri: Bagaimana Teknologi Informasi Mempengaruhi Industri Musik di Indonesia. Jurnal Pendidikan Sains dan Komputer, 2(01), 124-136.

Ruddin, I., Santoso, H., Indrajit, R. E., & Dazki, E. (2021). Big Entertainment's Film and Music Creation Design: Platform-Based Business Model Canvas and Enterprise Architecture. Capture: Jurnal Seni Media Rekam, 13(1).

Ruddin, I., Santoso, H., Indrajit, R. E., & Dazki, E. (2021). Contingency Planning in IT Risk Audit on Music Digital Recording Company. Journal of Music Science, Technology, and Industry, 4(2), 191-209.

Ruddin, I. (2023). Memilih Strategi Brand Management Yang Baik. Media Sains Indonesia.

Schjolberg, S. (2020). The History of Cybercrime (Vol. 13). BoD–Books on Demand.

Smith, P. R., & Zook, Z. (2019). Marketing communications: Integrating online and offline, customer engagement and digital technologies. Kogan Page Publishers.

Świątkowska, J. (2020). Tackling cybercrime to unleash developing countries′ digital potential. Pathways for Prosperity Commission Background Paper Series, 33, 2020-01.

Widijowati, D. (2022). Legal Complexity in Dealing with Cyber Crime in Indonesia. Research Horizon, 2(6), 597-606.

Younies, H., & Al-Tawil, T. N. E. (2020). Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). Journal of Financial Crime, 27(4), 1089-1105.