JOURNAL LA SOCIALE

VOL. 05, ISSUE 06 (1576-1586), 2024
DOI:10.37899/journal-la-sociale.v5i6.1367

Investigation of Cyber Crime in the Indonesian Legal Framework

Rusman[1], Ahmad Kamaludin[2]

[1]*Faculty of Law, Suryakancana University*
[2]*Faculty of Law, Islam Negeri Sunan Gunung Djati University*

**Corresponding Author: Rusman*
E-mail: drrusmanshmh@gmail.com

Article Info

Article history:
Received 12 June 2024
Received in revised form 24 July 2024
Accepted 7 August 2024

Keywords:
Crime
Cyber
Law
Regulation
Technology

Abstract

Cybercrime in Indonesia is influenced by complex factors such as technological advancement, anonymity, lack of security awareness, inequality of technological development, financial reasons, and low law enforcement capacity. The legal regulation of cybercrime is based on the current legal sources both in the Criminal Code and laws outside the Criminal Code. Some categories of cybercrime cases handled in the Electronic Information and Transaction Law include illegal contents, illegal access, illegal interception, data leakage and espionage, system interference, misuse of devices, and data interference. Cybercrime is a criminal offence that uses computers and the internet as a means. Legal reform in handling cybercrime must be carried out with a policy approach that contains value considerations. Criminal law reform in overcoming information technology crimes must be oriented towards a value approach. Cybercrime is a crime that uses computers or computer networks as the main tool. In Indonesia, there is no specific legal definition for cybercrime. Cybercrime can be in the form of unauthorised access, illegal contents, data leakage, trojan horses, and others.

Introduction

Information technology has developed very rapidly in various countries including Indonesia. Advances in information technology have a good influence on economic development and the rapid acquisition of information from around the world (Mohammad et al., 2023). Behind the benefits, advances in information technology also bring negative impacts, one of which is cybercrime, such as espionage, financial theft, and other cross-border crimes, at the international level. Warren Buffett places cybercrime as the most important issue for humanity and states that it poses a real threat to humanity.

Cybercrime in Indonesia has reached the highest number in the world, one of which is due to the high hacking activity in Indonesia, which uses internet facilities that are almost uncontrollable, as in 2021 internet users in Indonesia reached 202.6 million, in 2022 it reached 204.7 million (Mutia Annur, 2024) Meanwhile, in 2023-2024 it reached 221.5 million of the total population of Indonesia in 2023 (APJII, 2024; Chirzah & Ramadhan, 2023; Putri et al., 2022). Thus, resulting in increased victims of cybercrime such as *hacking; phishing; malware; ransomware; spyware; denial of service; identity theft; cyberstalking, fraud; online piracy; SQL injection; man-in-the-middle attack; botnet; cryptojacking.* According to cyber patrol data, cybercrime in Indonesia has been reported in 6,388 cases since 2019 until 22 May 2020 (Siber, 2020), while in 2021-2022 according to data in the e-MP Robinopsnal Bareskrim Polri there were 8,831 cases of cybercrime (Polri, 2022).

To prevent cybercrime, communities and governments need to have an in-depth understanding of cybercrime schemes and the contemporary and ongoing internet trends and behaviours of the perpetrators of these crimes (Butarbutar, 2023). Addressing this problem requires a multi-

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

disciplinary approach involving technology, law, and public awareness. On the legal front, strict law enforcement and adaptive regulatory updates are essential. Strengthening the capacity of law enforcement officers and international co-operation are also key in addressing this issue. The Indonesian government itself has incorporated the *Cyber Crime* Law into Law Number 11 of 2008 or often called the ITE Law, and hopes that Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 can overcome, reduce and stop cyber criminals (Rahman Najwa, 2024). In 2022 there was a hacking case committed by a hacker named Bjorka. This hacker hacked President Joko Widodo's document data, MyPertamina, KPU data, and sim card registration. In the following year, a hacking case committed by BreachForums hackers caused one million sample data to be accessed, the leaked information contained the population identification number (NIK), full name, date of birth, birth certificate number, blood type, religion, and marital status. The following year, a hacking case was carried out with the LockBit 3.0 Ransomware. Ransomware is a term for a type of malware that attacks data systems resulting in the National Data Centre (PDN) being hacked, disrupting services at a number of government agencies. In addition to the cyberattack on the PDN, BSSN also revealed that data belonging to the Indonesia Automatic Fingerprint Identification System or Inafis Polri was sold on the dark web. In addition, the hack also affected the Temporary National Data Centre 2 (PDNS2) which made the KIP Lecture system at the Ministry of Education and Culture, universities were instructed to postpone the Single Tuition Fee (UKT) payment deadline for Indonesia Smart Card (KIP Lecture) applicants who were accepted through the Achievement-Based National Selection (SNBP) and Test-Based National Selection (SNBT).

As stipulated in Law No. 19/2016, the main regulation in Indonesia governing activities in cyberspace including investigation and law enforcement actions related to cybercrime is regulated in the Law. However, there are challenges for investigators in the investigation of cybercrime regarding some of the above cases that are difficult to prove the crime because the perpetrator easily obscures or eliminates evidence quickly.

As in previous research conducted by Rio Armanda and Jeane Darc Noviayanti Manik on "Electronic Information Crimes in the Positive Legal Framework". This article provides an in-depth analysis of the legal issues faced after the enactment of Law Number 11/2008 on Electronic Information and Transactions (ITE Law), especially after several decisions of the Constitutional Court, covering issues such as legal certainty related to criminal provisions, protection of personal data, and criminal investigations. The research method used is normative juridical with a statutory and conceptual approach, which provides a strong theoretical foundation as well as in-depth regulatory analysis. This article also highlights the importance of personal data protection in online activities and the rights associated with privacy. In addition, the research takes into account socio-cultural and religious values in the application of cyber law in Indonesia, which are rarely discussed in the context of cyber law. However, the research is largely normative in nature with a statutory and conceptual approach, which means there is a lack of empirical data that can support the legal analyses presented. The article focuses heavily on the positive legal framework, perhaps lacking the practical implications of the implementation of the ITE Law on the ground as well as the perspectives of legal practitioners. The use of complex and technical legal terms may limit understanding for readers who do not have a strong legal background. In addition, this article may lack attention to the latest technological developments and how these affect the implementation of ITE Law, given the rapid changes in information and communication technology.

Meanwhile, as in previous research conducted by Sukinta on "The Role of the Police in Investigating the Crime of Spreading Fake News in Indonesia". This article provides an in-

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

depth analysis of research on the role of the police in investigating criminal offences of spreading fake news in Indonesia has several shortcomings that need to be considered. First, the socio-legal research approach used focuses more on the implementation of law in society and may lack depth in normative legal analysis. This could be a weakness if this research does not sufficiently explore the normative and theoretical aspects of the applicable law. Secondly, the scope of this research, which focuses on the role of the police, may not cover other relevant aspects, such as the social and economic impacts of spreading fake news and comparisons with other countries in handling similar cases. Third, the validity and representativeness of the data used is also a concern. If the data taken is not broad enough or only based on specific cases, the results of the study may not generalise well. Fourthly, although barriers and countermeasures have been identified, a more in-depth analysis of all barriers and countermeasure strategies may be needed to provide a more comprehensive picture. Finally, the conclusions and recommendations from this study may not be detailed or applicable, requiring more concrete and practical suggestions for future improvements.(Sukinta, 2020)

Overall, these two studies have their own strengths and weaknesses. The research by Rio Armanda and Jeane Darc Noviayanti Manik has advantages in analysing normatively and conceptually. However, the empirical and practical aspects are not accommodated. Meanwhile, the research conducted by Sukinta is more visible in terms of practical implementation in the field. These two studies are the basis for the author to perfect this research by collaborating between the two studies.

This research plays a crucial role in understanding the realm of cybercrime in Indonesia. It explores cybercrime categories, modus operandi, and the legal framework governing them in the Indonesian legal system. The main objectives of this research are to analyse the effectiveness of relevant laws, assess the level of legal protection provided, identify influencing factors, and detect challenges in law enforcement related to cybercrime. From the results of this analysis and evaluation, it is hoped that recommendations can be made to strengthen the legal framework to improve digital security and justice for information technology users in Indonesia.

Methods

Literature Study

The literature study presented is commendable for its effort to connect theories and legal perspectives related to the regulation of cybercrime within the Indonesian legal system. However, the content could benefit from a more comprehensive and nuanced exploration of relevant theories. Including a wider range of theoretical perspectives on cybercrime, such as criminological theories or theories of international law, might enrich the analysis. For instance, incorporating perspectives from global cybersecurity frameworks or comparing Indonesian regulations with those of other countries could provide a more robust understanding of the regulatory landscape. Additionally, referencing seminal works and recent studies in the field would offer a more balanced view and demonstrate the current state of research on cybercrime regulation.

Analysing Legislation

The analysis of legislation related to cybercrime in the Indonesian legal system is crucial for understanding the scope and effectiveness of the legal framework. The research should be more detailed in its examination of specific regulations and their practical implications. For example, it would be beneficial to assess how effectively current laws address emerging cyber threats and how enforcement mechanisms are implemented in practice. Analyzing recent legislative amendments or proposed reforms would also provide insight into how the legal system is

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

adapting to new challenges. Furthermore, comparing Indonesian legislation with international standards or best practices could highlight areas for improvement and suggest potential legal reforms.

Identification of Cyber Crime

The identification and definition of cybercrime offences are essential for understanding the scope of the research. The current discussion could be enhanced by providing a more detailed categorization of different types of cybercrime, including emerging threats like ransomware or cyber espionage. Clarifying the definitions and distinguishing between various forms of cybercrime would help in understanding their specific implications for the legal system. Additionally, integrating case studies or real-world examples of cybercrime incidents in Indonesia could illustrate how these offences manifest and impact society, thus offering a clearer picture of the challenges faced.

Normative Analysis

The normative analysis of the legal system is valuable for understanding the regulatory framework surrounding cybercrime. To strengthen this section, the research should delve deeper into how the norms and regulations are applied in practice. Examining the effectiveness of existing legal norms and their enforcement can provide insights into the practical challenges and limitations faced by the legal system. Comparing the normative framework with international standards or similar jurisdictions could reveal gaps or discrepancies in the Indonesian legal approach. Including perspectives from legal experts or practitioners might also enrich the analysis by offering practical insights into the application of these norms.

Theoretical Framework

The compilation of theories explaining the regulation of cybercrime is an important aspect of the research. To enhance this section, it would be beneficial to include a wider range of theoretical perspectives and explain their relevance to the Indonesian context. Incorporating theories from cybersecurity, international law, or comparative legal studies could provide a more comprehensive understanding of the regulatory landscape. Additionally, discussing how these theories inform policy and legislative developments in Indonesia would demonstrate the practical implications of the theoretical framework. Providing a critical analysis of how well the current theoretical approaches address the realities of cybercrime would also strengthen the discussion.

Drawing Conclusions

The conclusions drawn from the analyses should be detailed and well-supported by the findings of the research. It is important to ensure that the conclusions are not only reflective of the data but also provide actionable insights. The discussion should address how the current regulatory framework addresses the challenges identified and suggest specific improvements or areas for further research. Providing recommendations for policy changes, legislative reforms, or practical measures to enhance the effectiveness of cybercrime regulation would add value to the conclusions. Furthermore, discussing the implications of these findings for stakeholders, such as policymakers, law enforcement, and the public, would offer a more comprehensive view of the impact of the research.

Results and Discussion

Forms of *Cyber Crime*

Cybercrime has become a global phenomenon that has received serious attention from various parties. Vodymyr Golubev defines it as a new form of antisocial behaviour. Other terms used

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

to describe cybercrime include "*cyber space offence"*, new dimensions of high-tech crime, new dimensions and transnational crime, and new dimensions of white-collar crime (Akub, 2018).

Cybercrime, which arises because of the cybercommunity on the internet, has different characteristics from the previous two crime models. Some of the things that distinguish it include: 1) the scope of the crime; 2) the nature of the crime; 3) the perpetrators of the crime; 4) the mode of crime; and 5) the type of loss caused (Abidin, 2015).

Cybercrime is increasing due to the development and advancement of technology today, because in this digital era many aspects of daily life depend on technology and internet connectivity. Cybercrime comes in many forms and the actions taken by the perpetrators are varied, which include:

Table 1. Form of Cybercrime

Term	Definition	Reference
Hacking	Refers to the process or activity in which a person, commonly called a hacker, attempts to manipulate, access, or alter information contained in a computer system or network, often without the owner's permission or knowledge.	Hapsah, F., & Nasution, T. (2023).
Phishing	A mode of online fraud to steal personal data such as name, age, address, account data (username and password), and financial data (credit card and account information) by tricking the victim.	Rompi, S., & Muaja, R. (2021).
Malware	Malicious software specifically designed to enter a system without its owner knowing and stay there for a long time. Malware usually disguises itself as a safe program to trick users.	Sari, A. (2024).
Ransomware	A type of malware that encrypts data or prevents access to the victim's system and demands a ransom to unlock the system or restore the data.	Ramadhan, I. (2023).
Spyware	Malicious software intended to collect data from a device or computer without the user's knowledge or consent. Collected data can be sent to private companies or individuals to deliver unwanted advertisements or spread harmful viruses.	Septian, R., et al. (2024).
Denial of Service	A type of attack on a computer network that aims to deplete the power of computer equipment, disrupting the network. When using the TCP/IP protocol, the attack often begins with a three-way handshake.	Sutarti, A., & Khairunnisa, N. (2017).
Identity Theft	When an offender presents himself or herself as someone else, often using stolen credentials or a false identity, to commit fraud or gain access to benefits.	Mahmud, A. (2019).
Cyberstalking	The act of threatening, harassing, or annoying someone through various electronic communications, especially with the intention of putting the recipient in fear of illegal actions or harm to themselves or their family members.	Zakaria, A., et al. (2022).
Fraud	The use of a position by someone to enrich themselves through deliberate misuse or	Septian, R., et al. (2024).

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

	misappropriation of organizational assets or resources.	
Online Piracy	The unlawful act of copying and distributing copyrighted content over the internet without the copyright owner's permission.	
SQL Injection	A technique for exploiting applications that use databases for data storage by injecting malicious SQL code.	Bastian, M., et al. (2017).
Man-in-the-Middle Attack	A security threat that exploits weaknesses in communication networks to steal or manipulate information transmitted between two parties.	Firmansyah, T. (2023).
Botnet	A distributed platform for illegal activities such as deploying DoS attacks, posing a serious threat to cyber security.	Shidik, Y., & Karima, R. (2011).

These cybercrimes are a new phenomenon that is different from traditional crimes, this is in line with the rise of crimes that currently occur through technological sophistication. So that the actions of the perpetrator in committing cybercrime make it possible for the perpetrator to become antisocial because the perpetrator does not directly face his victim but through cyberspace, this is in accordance with the theoretical statement said by Vodymyr Golubev.

An example of a cybercrime case that is currently rampant is data theft such as what happened to the national data centre. In addition, based on data from the National Police, there are several cases of crime from the 2021 period, the number of prosecutions is 612 cases and in 2022 there are 8,831 cases. From 1 January to 22 December 2022 the National Police took action against several types of cases related to cybercrime in Indonesia, including: authentic data manipulation in 3,723 cases, electronic media fraud in 2,131 cases, cybercrime in 1,098 cases, defamation through electronic media in 835 cases, unauthorised access to the system in 358 cases, online gambling in 164 cases, threatening electronic media in 145 cases, insults through electronic media in 59 cases and hate speech in 43 cases. (Polri, 2022).

Factors Influencing *Cyber Crime*

The increase of *cybercrime* in Indonesia certainly has a background or factors that influence the occurrence of this criminal offence. The level of *cybercrime* in Indonesia is influenced by a number of complex factors involving technological, social, economic, and legal aspects and can come from within humans or internal factors and can also come from external influences or external factors. Factors that can influence the level of *cybercrime* in Indonesia include:

Firstly, due to technological advances, with the advancement of technology and the availability of the internet, *cyber* criminals have more opportunities to carry out attacks. Internet connectivity on devices and the widespread use of information technology open up opportunities for cyber criminals to carry out actions, such as data theft, system destruction, and other disruptions. The increasing number of individuals connected to the internet increases the potential victims and expands the space for cybercriminals. (Mahira Dewantoro & Setiawan, 2023).

The second is anonymity, which is the ability to carry out attacks anonymously is one of the most interesting aspects of cybercrime. Cyber criminals can use techniques such as virtual private networks (VPNs) to hide their digital footprint. Thus, the ability of perpetrators to hide their identities and traces makes them difficult to detect and apprehend. (Mahira Dewantoro & Setiawan, 2023).

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

Furthermore, there is a lack of security awareness of *cybercrime*, because the level of public awareness in Indonesia and other related parties such as institutions still do not fully understand the risks of crimes originating from a technology that is used daily. (Bodhi & Tan, 2022). Finally, the capacity of law enforcement in handling cybercrime is still weak. Lack of understanding and technical expertise in conducting investigations into *cyber* attacks can be an obstacle in the law enforcement process so that there are still many cases of this criminal offence and many people are still affected by *cybercrime* that causes various losses.

Legal Arrangement of *Cyber Crime*

The United Nations (UN) Congress encourages its member states to combat cybercrime through criminal law enforcement. This means defining what constitutes a cybercrime and what penalties will be given to the perpetrators (Nuristiningsih, 2023).

The handling of cybercrime in Indonesia is based on various laws, both in the Criminal Code (KUHP) and outside the KUHP. These laws do not only apply to acts that occur in Indonesia or are committed by Indonesian citizens, but also cover acts that occur outside the territory of Indonesia (Nuristiningsih, 2023).

Articles in the Criminal Code become the main reference to understand and handle cybercrime in Indonesia. Articles in the Criminal Code become the main reference to understand and handle cybercrime in Indonesia: (1) Article 362 of the Criminal Code (KUHP) regulates the offence of theft;(2) Article 369 of the Criminal Code (KUHP) contains legal provisions on Extortion, Threatening; (3) Kitab Undang-Undang Hukum Pidana (KUHP) Article 372 on the regulation of Embezzlement; (4) Kitab Undang-Undang Hukum Pidana (KUHP) Article 386 on the regulation of fraudulent acts; (5) Kitab Undang-Undang Hukum Pidana (KUHP) Article 506 on the criminal offence of Public Order Violators; (6) Criminal Code (KUHP) Article 382 on Business Competition; (7) Kitab Undang-Undang Hukum Pidana (KUHP) Article 383 on Fraud in buying and selling

Several cybercrime cases have been resolved with reference to the provisions of the ITE Law (Articles 27 to 35):

Article 27 Illegal Contents

Content that violates decency (Pornograph); *Computer-related betting*; Defamation and libel; *Extortion* and *threats*.

Article 28 Illegal Contents

Consumers can become victims of fraud and suffer financial losses due to false and misleading news circulating in electronic transactions. (*Service Offeredfraud*); Information designed to trigger negative sentiments and divisions among the public. (SARA).

Article 29 Illegal Contents

Transmission of Electronic Information and/or Electronic Documents containing threats of violence or fear aimed at certain individuals.

Article 30 Illegal Access

Perform acts of unauthorised and unauthorised access to computers and/or electronic systems belonging to others in any way. Perform illegal access actions to retrieve and copy Electronic Information and/or Electronic Documents belonging to others without the consent and knowledge of the owner. Perform acts of illegal access to computers and/or electronic systems by breaking into, breaking through, bypassing, or breaching their security systems.

Article 31 Illegal Interception

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

Perform acts of interception or eavesdropping to spy on the activities and electronic communications conducted by others through their computers or electronic systems. Perform interception actions to intercept and monitor non-public electronic communications in progress on another person's computer or electronic system, whether or not altering the content of the communication or altering, removing, or stopping the transmission of the communication.

Article 32 Data Leakage and Espionage

Perform actions to change, add, or reduce the content of Electronic Information and / or Electronic Documents belonging to others or belonging to the public in an unlawful manner.

Article 33 System Interference

Take any action that results in paralysing or stopping the operation of the Electronic System in whole or in part.

Article 34 Misuse of Device

Provide or distribute malware, viruses or other malicious programmes designed to damage, disrupt or steal data from Electronic Systems, with the aim of facilitating *cybercrime.*

Article 35 Data Interference

Every person intentionally and without rights or against the law manipulates, creates, changes, removes, destroys Electronic Information and/or Electronic Documents with the aim that the Electronic Information and/or Electronic Documents are considered as authentic data. Deliberately and without rights or unlawfully accessing another person's Computer and/or Electronic System by any means. Deliberately and without rights or unlawfully accessing a Computer and/or Electronic System by any means with the aim of obtaining Electronic Information and/or Electronic Documents. Intentionally and without rights or unlawfully accessing a Computer and/or Electronic System in any way by violating, breaking through, exceeding, or penetrating the security system.

Article 31 Illegal Interception

Perform interception or wiretapping actions to steal Electronic Information and/or Electronic Documents contained in a computer or electronic system belonging to another person. Interception of illegal acts to intercept and monitor the transmission of confidential or non-public Electronic Information and/or Electronic Documents belonging to another person, either without causing alteration, or causing alteration, omission, and/or termination of the transmission of such data.

Article 32 Data Leakage and Espionage

Perform acts of manipulation of electronic data and/or electronic documents belonging to others or belonging to the public without legal rights and permissions, with the aim of harming or misleading.

Article 33 System Interferenc

Perform actions aimed at damaging or disabling electronic systems, thereby disrupting activities and operations that depend on such systems.

Article 34 Misuse of Device

Providing technological tools, such as computer hardware or software, that are specifically designed or modified to help commit cybercrime, such as stealing data, spreading malware, or hacking.

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

Article 35 Data Interference

A person intentionally and without rights or against the law performs acts of manipulation, creation, alteration, removal, or destruction of Electronic Information and/or Electronic Documents to deceive and mislead other parties.

Conclusion

Cybercrime is a criminal offence that uses computers and the internet as a tool, regardless of national borders. The form of *cybercrime* can be differentiated based on the activities and motives of the perpetrators. In Indonesia, legal regulation related to *cybercrime* is carried out through the Criminal Code and special laws outside the Criminal Code. However, there are still challenges in law enforcement and digital security protection due to complex factors such as technological advances, anonymity, and low awareness of security.

Legal reform in handling cybercrime needs to be carried out with a policy approach that contains value considerations. Criminal law reform related to information technology crime must be oriented towards a value approach that can accommodate technological developments and the need to protect society from the threat of *cybercrime*. In addition, it is important to continue to conduct research on *cybercrime* to analyse the effectiveness of the law, evaluate legal protection, and identify challenges in law enforcement in the digital era.

Cybercrime in Indonesia includes various categories of cases such as illegal contents, illegal access, data leakage, and others. Although the Indonesian government has implemented laws related to *cybercrime*, an interdisciplinary approach is still needed for effective prevention and law enforcement. Thus, protection of digital security and law enforcement against *cybercrime* are important to maintain security and order in cyberspace.

References

Akub, M. S. (2018). Pengaturan Tindak Pidana Mayantara (Cyber Crime) dalam Sistem Hukum Indonesia. *World Development, 1*(1), 1–15.

APJII. (2024). *APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang*. Retrieved July 17, 2024, from apjii.or.id website: https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

Bastian, A., Sujadi, H., & Abror, L. (2017). Analisis Keamanan Aplikasi Data Pokok Pendidikan (Dapodik) Menggunakan Penetration Testing Dan Sql Injection. *Infotech Journal*, 65–70.

Bodhi, S., & Tan, D. (2022). Keamanan Data Pribadi Dalam Sistem Pembayaran E-Wallet Terhadap Ancaman Penipuan Dan Pengelabuan (Cybercrime). *UNES Law Review, 4*(3), 297–308. https://doi.org/10.31933/unesrev.v4i3.236

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, DanPerkembangannya. *Technology and Economics Law Journal, 2*(2), 299–317.

Chirzah, D., & Ramadhan, R. A. (2023). Cyber War Ancaman Pada Keamanan Nasional. *Jurnal Trends, 01*(01), 9–18. https://doi.org/https://doi.org/10.56772/trends.v1i1.289

Abidin, D. Z. (2015). Kejahatan dalam Teknologi Informasi dan Komunikasi. *Jurnal Processor*, *10*(2), 509-516.

Firmansyah, D. (2023). Penerapan Teknologi Blockhain Untuk Mengatasi Serangan Man In The Middle. *Journal Science Informatica and Robotics, 1*(1), 73–80.

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

Hapsah, Z. F., & Nasution, M. I. P. (2023). Analisis Tingkat Keamanan Data Perusahaan Yang Rentan. *Jurnal Manajemen Dan Akuntansi*, *1*(2), 338–343.

Mahira Dewantoro, N., & Setiawan, D. A. (2023). Penegakan Hukum Kejahatan Siber Berbasis Phising dalam Bentuk Application Package Kit (APK) Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *Bandung Conference Series: Law Studies*, *3*(2), 892–900. https://doi.org/10.29313/bcsls.v3i2.7247

Mahmud, R. (2019). Pencurian Identitas Kategori & Kasus. *Cyber Security Dan Forensik Digital*, *2*(1), 38–42. https://doi.org/10.14421/csecurity.2019.2.1.1421

Mohammad, A., Mustam, A., Hukum, M., Islam, U., Surakarta, B., Criminal, D., & Pendahuluan, I. (2023). Memerangi Kejahatan Siber di Indonesisa : Analisis Regulasi Hukum Pidana yang berlaku dan tantangannya. *Jurnal Gema : Disiplin Ilmu, 35*(01), 10–14.

Mutia Annur, C. (2024). *Ada 30 Kasus Bullying Sepanjang2023, Mayoritas Terjadi di SMP*. Retrieved February 20, 2024, from databoks.katadata.co.id website: https://databoks.katadata.co.id/datapublish/2024/02/20/ada-30-kasus-bullying-sepanjang-2023-mayoritas-terjadi-di-smp

Nuristiningsih, D. (2023). Upaya Penal Dan Non Penal Dalam Menanggulangi Tindak Pidana Teknologi Informasi. *Majalah Keadilan*, *23*, 62–90.

Polri, P. B. (2022). *Kejahatan Siber di Indonesia Naik Berkali-kali Lipat*. Retrieved July 17, 2024, from pusiknas.polri.go.id website: https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat

Putri, A. W. O. K., Aditya, A. R. M., Musthofa, D. L., & Widodo, P. (2022). Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus: Predator). *Global Political Studies Journal*, *6*(1), 35–46. https://doi.org/10.34010/gpsjournal.v6i1.6698

Rahman Najwa, F. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dah Hukum*, *2*(1), 8–16.

Ramadhan, G. (2023). Perlindungan Hukum Bagi Korban Ransomware Wannacry Tindak Pidana Ransomware. *Jurnal Kajian Kontemporer Hukum Dan Masyarakat*, 1–17. https://doi.org/10.11111/dassollen.xxxxxxx

Rompi, T., & Muaja, H. S. (2021). Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan. *Lex Privatum*, *9*(4), 183–192.

Sari, R. P. (2024). *Apa itu Malware? Jenis dan Cara Pencegahannya*. Retrieved July 24, 2024, from Cloud Computing Indonesia website: https://www.cloudcomputing.id/pengetahuan-dasar/apa-itu-malware-jenis

Septian, A., Alfiansyah, T., Abdulla, A. D., Sutiawan, H., Ega, D. A., Fauzi, … Saepudin, T. H. (2024). Analisis Tingkat Keamanan Data Pada Salah Satu Kantor Perpajakan Di Bekasi Yang Rentan Terhadap Serangan Cyber Dalam Sistem Keuangan. *Jurnal Humaniora, Sosial Dan Bisnis*, *2*(7), 711–718.

Shidik, G., & Karima, A. (2011). Framework Untuk Mendeteksi Botnet Kraken Dan Conficker Pada Jaringan Komputer. *Seminar Nasional Teknologi Informasi & Komunikasi Terapan*, 1–9.

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

Siber, P. (2020). Jenis kejahatan siber di Indonesia, 2019-2020.

Sukinta, S. (2020). *Peran Kepolisian Dalam Melakukan Penyidikan Tindak Pidana Penyebaran Berita Bohong di Indonesia.* Online Administrative Law & Governance Journal, 3(3), 2621–2781. https://doi.org/https://doi.org/10.14710/alj.v3i3.554%20%20-%20%20568

Sutarti, S., & Khairunnisa, K. (2017). Perancangan dan analisis keamanan jaringan nirkabel dari serangan DDOS (Distributed Denial Of Service) berbasis Honeypot. *PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer*, *4*(2).

Zakaria, H., Samsoni, & Mulyoto, A. (2022). Cyberstalking Sebuah Kejahatan Di Dunia Maya Yang Berimplikasi Hukum. *AMMA : Jurnal Pengabdian Masyarakat, 1*(07), 823–829.

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)