International Journal of Society Reviews (INJOSER) e-ISSN: 3030-802X
Vol. 1 No. 11 2024, pages: 1548~1561

INDONESIAN CRIMINAL LAW REFORM IN THE FACE OF CYBERCRIME

Loso Judijanto *[1]
IPOSS Jakarta, Indonesia
losojudijantobumn@gmail.com

Melyana R Pugu
Universitas Cenderawasih
puguratana@yahoo.com

Yuarini Wahyu Pertiwi
Universitas Bhayangkara Jakarta Raya
yuarini.wp@dsn.ubharajaya.ac.id

Abstract

Criminal law reform in the face of cybercrime is a critical issue that requires attention in Indonesia. The research method used in this study is literature review. The purpose of this study is to evaluate the effectiveness of the current ITE Law and identify aspects that require improvement to optimise law enforcement against cybercrime. The results show that the current ITE Law requires adjustments to include more specific definitions and clear boundaries to avoid multiple interpretations and misuse. There is a need to update and enhance the law with higher standards related to human rights and freedom of expression. In addition, Indonesia's information technology infrastructure and human resources require improvement through investment and training to effectively address cybercrime challenges. International cooperation is also an important element of this research, which concludes that Indonesia should participate more actively in inter-state conventions and cooperation to strengthen its response to cross-border cybercrime. Therefore, this research suggests that legal reform, capacity building, and international cooperation are necessary to support Indonesia's efforts in dealing with cybercrime.

Keywords: Reform, Criminal Law, Cyber Crime.

Introduction

In the era of globalisation and the information technology revolution, the internet has turned into a space that not only provides convenience and efficiency, but also a new arena for various forms of crime known as cybercrime. Cybercrime is an unlawful act where computers and internet networks are used as tools, targets, or places of crime. These activities include, but are not limited to, online fraud, account hijacking, identity theft, and the spread of computer viruses. (Ishak et al., 2023).

In Indonesia, the rapid growth of internet users creates a vulnerability to cyber crime incidents. In line with these digital advances, cybercrime has become a crucial

[1] Correspondence author

issue that requires a fast and adaptive legal response. (Raharjo, 2021). Indonesia's criminal law, codified in the Kitab Undang-Undang Hukum Pidana (KUHP), is more than a century old and was not designed to accommodate the new types of crimes that have emerged with technological advances (Budianto & Wulandari, 2020).

These crimes not only impact individuals through identity theft, online fraud, and privacy violations, but also threaten the security and stability of nations and economies through cyberattacks on critical infrastructure and financial systems. (Koto, 2021). In this case, the harm caused by cybercrime not only affects the victims directly, but it can also reduce public trust in digital technology as a thread of modern life. (Imran, 2023).

However, Indonesia's current criminal laws, including the Electronic Information and Transaction Law (ITE), do not appear to be strong enough to address and effectively prevent and prosecute the growing number of cybercrimes. (Suhendi & Asmadi, 2022).. Many criticisms point to the vagueness and limitations in the definition and scope of the existing law, which creates opportunities for criminals to escape the law. In addition, the challenges of updating and adapting laws to technological developments point to the urgency of reforms that focus not only on increasing sanctions, but also on prevention, education and international co-operation, given that cybercrime is often transnational. Therefore, increasing legal capacity and law enforcement are critical elements in keeping Indonesia's digital space safe and reliable. (Puspitosari, 2020).

Furthermore, to address the complexity of cybercrime, a dynamic legal framework that can adapt to rapid technological developments is required. Criminal law reform should include the drafting of cybercrime-specific laws with clear, specific, and detailed definitions for various cyber offences, including but not limited to cyberattacks, online fraud, establishment of crimes against data security, and protection of personal data. (Nurahman, 2020). This is important to reduce legal ambiguity and provide legal certainty, both for perpetrators, victims, and law enforcement officials. It is also important to establish a law enforcement framework that allows for swift and effective enforcement, as well as cross-agency and cross-country co-operation to address the transnational nature of many cybercrimes (Nugraha et al., 2020). (Nugraha et al., 2021).

In terms of prevention, public education is also an important factor in reducing the risk of cybercrime. The public should be made aware of cyber threats and how to protect themselves from such attacks. In addition, investment in cybersecurity technology and infrastructure, as well as the development of a national cyber force, are important steps to strengthen defences against potential cyberattacks. (Zulhidayat, 2020). In addition, the involvement of the private sector, especially digital system and application providers, is needed to ensure that security principles are applied starting from the system design stage (Yusni & Sigalingging, 2020). (Yusni & Sigalingging, 2022)..

In the global context, the need for international cooperation to strengthen cyber law and security cannot be ignored. Indonesia's criminal laws must be synchronised and compatible with international conventions and norms to ensure that the extradition

process, mutual legal assistance, and information exchange can run effectively. (Listiyanto & Arpangi, 2021).

Finally, criminal law reform in the context of cybercrime in Indonesia is not only an urgency, but also a necessity that must be realised immediately. This progressive step will put Indonesia in a more formidable position to tackle cybercrime and protect the public and national assets in the ever-evolving digital space. (Azizah et al., 2021).

The adaptation of criminal law in Indonesia to technological developments is a necessity that cannot be delayed, given the rapid evolution of digital technology and the emergence of increasingly complex cybercrime threats. In this context, legal adaptation requires legislative updates that are able to reach new problems caused by technological developments. (Melati et al., 2021). This includes the introduction of new categories of crimes that were previously undefined in conventional legal tools, such as cyberattacks on critical infrastructure, digital identity theft, and the spread of malware. The need to update current regulations and laws is not a one-off, but an iterative process that requires continuous monitoring and adjustment to technological trends and cybercrime modus operandi. (Hartati et al., 2022)..

On the other hand, adjusting the criminal law also involves increasing the institutional capacity and human resources associated with law enforcement. This means that it is not enough just to update regulations, but it must also be accompanied by an increase in the competence of law enforcement officials in facing these new challenges. (Takdir & Fitriasih, 2023). This capacity building includes training on information technology, digital forensics, and international co-operation to deal with cybercrime that crosses national borders. This overall approach is expected to not only improve the effectiveness of handling cybercrimes that have already occurred, but also develop proactive prevention mechanisms to reduce the potential for crimes to occur in the digital space. (Suprapto et al., 2023)..

Such reforms should address current legal barriers, as well as strengthen the legal framework for personal data protection, effective prosecution, and fair enforcement. (Yuhernawa & Fakrulloh, 2021).

As such, this study will specifically explore the scope of cybercrime, deconstruct legislative limitations, and articulate the need for comprehensive reform of Indonesia's criminal law. By conducting an in-depth literature review, this study aims to present a framework for criminal law reform that is expected to provide more effective tools for handling cybercrime, while providing justice for all parties involved.

Research Methods

The method used in this research uses a literature review. The literature review method is a methodological approach used to collect, review and analyse existing information related to a topic or research question. (Nesset et al., 2024).. Literature research does not involve the collection of primary data through experiments or direct

observation, but rather focuses on the utilisation of written sources such as books, journal articles, research reports, and official documents (Teixeira & Carvalira, 2002). (Teixeira & Carvalho, 2024).. The purpose of literature research is to gain a thorough understanding of what is already known about a topic, identify consensus and differences in the existing literature, and find gaps or unanswered research questions. (Abdul et al., 2024).

In practice, desk research is often an important foundation of scientific research, providing context and justification for further research. In addition, it can serve as a valuable self-study in understanding and mapping the landscape of knowledge on a subject.

Results and Discussion

Definition and Scope of Cybercrime

Cybercrime, or computer crime, refers to illegal activities committed using information and communication technology, particularly the internet and computers. (Barlian & Herista, 2020).. These crimes involve the use of computer systems or networks to commit crimes such as stealing personal information, manipulating data, or damaging digital infrastructure. Cybercrime not only compromises the privacy of individuals and organisations but can also threaten national security and economic stability. With advances in technology, the methods and techniques of cybercriminals are becoming increasingly sophisticated, complicating detection and prevention efforts by law enforcement and cybersecurity specialists. (Pansariadi & Soekorini, 2023)..

The types of cybercrime vary and continue to evolve over time. Some of the most common examples of cybercrime include phishing, where attackers send legitimate-looking emails to steal sensitive information such as usernames, passwords, and credit card details. (Anwar, 2023). Malware, which is malicious software installed without the user's knowledge to steal data or damage the system. Ransomware is a type of malware that encrypts the victim's data and demands a ransom to restore data access. In addition, there are also denial of service (DoS) attacks that aim to paralyse a website or service by flooding the server with overwhelming traffic so that the service cannot be accessed by legitimate users. These crimes are just some of the forms of cybercrime that often occur, and each type has variations and complex methods. (Angga et al., 2023)..

The development of cybercrime in Indonesia shows an upward trend. With the growing internet penetration and digitalisation of various aspects of people's lives, Indonesia has become an easy target for cyber criminals. Various cases, ranging from online fraud, identity theft, to ransomware attacks on government and private institutions, have become a major concern. (Nurkholim, 2020). The National Cyber and Crypto Agency (BSSN), as the agency responsible for national cybersecurity, continues to improve its capacity and capability in dealing with increasingly sophisticated cyber

threats. However, the challenges remain great considering that cyber criminals also continue to develop the methods and technologies they use (Manullang et al., 2020). (Manullang et al., 2023)..

Globally, cybercrime is also growing rapidly and becoming a serious transnational threat. International organisations such as Interpol and various national cybersecurity agencies in various countries are warning about the increase in cyberattacks, especially in the midst of the COVID-19 pandemic that is pushing economic and social activities into the digital space. (Darma, 2021). Cyberattacks are not only designed to steal data or money, but also aim to disrupt critical infrastructure and public services, indicating that the impact of cybercrime is not only economic but also socio-political. In the face of this threat, international co-operation and information sharing between countries as well as between institutions are seen as key ingredients in a global cybercrime prevention and response strategy. (Siregar & Sinaga, 2021).

As such, cybercrime has become a serious and growing threat affecting both individuals and institutions around the world. In Indonesia, the rise of cybercrime has followed the growth of internet usage and digitalisation, posing challenges to the security of personal data and critical infrastructure. Efforts to tackle cybercrime in Indonesia are still being enhanced through co-operation between government agencies such as BSSN.

Globally, cybercrime has evolved into a transnational threat that requires strong international coordination and co-operation to tackle effectively. The COVID-19 pandemic has accelerated digital transformation and at the same time increased the risk of cyber-attacks (Nawawi et al., 2023). These attacks are not only aimed at financial gain but also have the potential to destabilise economies and politics. (Damayanti & Ismowati, 2021).

Finally, both in Indonesia and globally, a multifaceted approach that involves strengthening cybersecurity, educating the public, and co-operation between countries and agencies is crucial. These efforts should focus on prevention, early detection, and rapid, coordinated response to reduce the impact of cybercrime.

Analysis of Indonesian Criminal Law on Cyber Crime

The Electronic Information and Transaction Law (UU ITE) is a regulation designed to govern and control the use of and transactions conducted through electronic systems in Indonesia. Enacted in 2008, UU ITE aims to provide a legal framework that supports the development of information and communication technology and ensures that electronic transactions are conducted within a safe and legal framework. (Mahardhika, 2021). This law covers various aspects ranging from electronic transactions, digital information dissemination, to handling cybercrime. Its special provisions cover aspects such as the use of electronic data as legal evidence, copyright

protection in the digital realm, and sanctions for cybercriminals who violate privacy and information security. (Ishak et al., 2023).

Changes and supplements to the ITE Law also continue to be made to adjust to the dynamics and development of technology and the needs of society. For example, the revisions made in 2016 included changes to several articles to further clarify certain definitions and limitations, as well as increase personal protection against defamation through electronic media. (Lindsey & Pausacker, 2020). In addition, there are other regulations that support the ITE Law such as regulations on broader internet governance and the administration of electronic systems and transactions. The Indonesian government, through the Ministry of Communications and Informatics, and other relevant agencies, continues to work towards the enactment of these regulations to ensure safety and fairness in the digital space, as well as to encourage people to use information technology responsibly and safely. (Adhi & Soponyono, 2021).

However, the ITE Law is not free from controversy and criticism, especially with regard to concerns over potential abuses in law enforcement that could limit freedom of expression and opinion. (Azhari, 2024). Certain articles in the ITE Law, such as those relating to defamation, are often questioned for their subjective application and can be used to silence criticism. In response, the government and Parliament have been discussing further revisions to strike a balance between legal protection from cybercrime and human rights, particularly in terms of freedom of speech in the digital space. (Putri et al., 2024). These revision efforts reflect the need to continuously refine regulations to keep up with technological developments and societal needs, as well as to avoid potential abuse. (Trisiana & Utami, 2022)..

In conclusion, Indonesia's ITE Law and its suite of related regulations are key components in the country's efforts to regulate and protect the national cyberspace from cybercrime and facilitate secure electronic transactions. Despite challenges and controversies related to the implementation and interpretation of certain articles, iterative efforts through regulatory revisions and adjustments demonstrate a commitment to the creation of a digital environment that is safe, fair and supportive of technological development and individual expression. In a dynamic digital landscape, dialogue and cooperation between the government, private sector, academia, and civil society are essential in ensuring that the regulations continue to be relevant and effective.

Basic Principles of Criminal Law in the Cyber Context

In the context of regulations such as the ITE Law, the principles of legality, proportionality, and adaptability are essential in maintaining a balance between legal security and individual freedom. Legality ensures that any form of regulation must have a clear legal basis and be officially communicated to the public, so that everyone knows what the law requires or prohibits. (Fadhil, 2023). Proportionality ensures that legal or

regulatory actions do not exceed what is necessary to achieve legitimate objectives, keeping the application of the law fair and not repressive. Adaptability refers to the ability of the law to adjust to changing conditions and technology, which is vital given the rapid development of information technology. (Khatrine, 2024).

In the application of the ITE Law in Indonesia, the balance between these principles is often a topic of debate. The legality of articles in the law is sometimes questioned, especially when they are deemed ambiguous or unclear in legal practice. Proportionality is also a major concern, with critics arguing that some articles have sanctions that are too severe or go too far in interfering with personal freedoms, as seen in cases of misuse of the defamation provisions (Supeno & Krismiyaryar). (Supeno & Krismiyarsi, 2023). Adaptability becomes particularly relevant here, as ITE Law needs to be constantly updated to remain effective in the ever-changing digital age and adapt to the latest needs and challenges in cyberspace. However, the challenge in implementing this adaptability lies in the speed with which the legislature can effectuate change and the consensus that must be built around such change. (Raharjo, 2021).

In comparing the criminal law systems of various countries, including Indonesia, with those of other countries, there are various approaches to regulating online crime. A number of countries, such as the United States and European Union countries, have detailed legal frameworks to deal with cybercrime, with specialised institutions established to combat this phenomenon. (Wahyuningsih et al., n.d.).. In the US, for example, laws such as the Computer Fraud and Abuse Act (CFAA) define and provide penalties for various forms of cybercrime. In the European Union, the General Data Protection Regulation (GDPR) places a strong emphasis on personal data protection and online security, with severe sanctions for violations. In both of these examples, the law was created with a focus on protecting individual rights and property, and paying attention to the concepts of fairness and proportionality in law enforcement. (Budianto & Wulandari, 2020).

In contrast to countries that have focused more on legislative reform and specialisation of existing law enforcement agencies, Indonesia is still in the process of achieving an ideal system for dealing with cybercrime. Indonesia, through the ITE Law, has made positive steps in the criminal law framework to tackle cybercrime, but criticisms continue to arise around the clarity and proportionality of certain articles. (Koto, 2021). Experiences from other countries can provide insights into how Indonesia can improve its EIT Law, particularly in ensuring that the law stays up to date with technological developments and tackles cybercrime more effectively while still protecting human rights. When comparing Indonesia's criminal law system with other countries, it is important to consider not only the differences in regulation, but also the social, political, and cultural contexts that influenced the formulation of the law. (Imran, 2023).

Adapting criminal law policies to address cybercrime is key to supporting a safe and fair digital environment. This involves balancing the prevention and prosecution of crime with the protection of privacy and freedom of expression. (Suhendi & Asmadi, 2022).. Positive examples from various legal systems demonstrate the importance of a dynamic legislative framework that can respond quickly to changing technology and social trends. In addition, international collaboration and continuous policy updates are crucial in addressing the growing transnational crime in cyberspace. (Puspitosari, 2020).

In drawing lessons from criminal law systems in other countries, Indonesia could endeavour to find solutions that strike a balance between cybersecurity and human rights. This could include improving ambiguous provisions in the ITE Law, increasing the capacity of law enforcement in dealing with cybercrime, and strengthening international cooperation in tackling cross-border cyber threats. (Nurahman, 2020). The integration of a multidisciplinary approach is also important, where inputs from information technology, law, and civil society are all considered in making policy. By capitalising on the strengths and addressing the challenges of the criminal justice system, Indonesia can move forward in creating a safe and supportive digital space for all its citizens, and make a significant contribution to the global fight against cybercrime. (Zulhidayat, 2020).

The Strengths and Weaknesses of Indonesian Criminal Law in the Face of Cybercrime

The strength of Indonesia's criminal law in dealing with cybercrime in general can be seen from the legal framework that has been prepared to regulate activities in the digital realm, specifically through the Electronic Information and Transaction Law (UU ITE). This law is the foundation that regulates aspects such as electronic transactions, digital copyrights, and insults and defamation on the internet, which shows Indonesia's seriousness in addressing cyber challenges. (Emaliawati, 2024). The existence of the ITE Law signifies a relatively strong legal basis to protect the public from various forms of cybercrime. In addition, another strength lies in the efforts to increase the capacity of law enforcement officials through continuous training and the establishment of specialised units, such as the Directorate of Cyber Crime in the Indonesian National Police, which shows the government's initiative in strengthening law enforcement against cybercrime (Fitran & Santiago, 2024). (Fitran & Santiago, 2022)..

However, there are several weaknesses in Indonesian criminal law in addressing cybercrime that need further attention. First, the vagueness and inconsistency in the application of several articles in the ITE Law are often criticised. These articles can sometimes be interpreted broadly, potentially leading to legal uncertainty and abuse of power. Secondly, despite efforts to increase the capacity of law enforcers, there are still constraints in terms of resources, be it personnel with specific expertise in cybercrime, as well as facilities and technology for investigations (Hamanduna & Widjanarki, 2014). (Hamanduna & Widjanarko, 2023).. Without solutions to these two weaknesses, it will

be difficult for Indonesia to optimise its law enforcement in the face of increasingly sophisticated and cross-jurisdictional cybercrime, requiring a comprehensive strategy and increased international cooperation. (YULIANTO & SUGIRI, 2022)..

Furthermore, to overcome these weaknesses, there is a need for a comprehensive revision and improvement of the ITE Law with more emphasis on fulfilling human rights standards and freedom of expression, and avoiding multiple interpretations that can lead to the restriction of civil liberties. These changes are expected to provide better legal clarity, reduce the potential for abuse, and increase confidence for the public and digital businesses that their activities are protected by fair and measurable laws. (Prasetyo & Hidayah, 2020). In addition, increasing resources should be prioritised, by allocating sufficient budget for information technology infrastructure development, increasing training for law enforcement, and establishing closer cooperation with cyber experts, security practitioners, and international institutions that have the capacity to combat cybercrime. (Listiyanto & Arpangi, 2021)..

In the international context, given the transnational nature of cybercrime, Indonesia also needs to be active in cross-border law enforcement efforts. This includes signing and ratifying international conventions related to cybercrime, such as the Budapest Convention on Cybercrime, and enhancing co-operation with law enforcement agencies in other countries in the exchange of information and extradition of offenders (Azizah et al., 2021). (Azizah et al., 2021). This increased cooperation is important to address legal challenges caused by jurisdictional differences and ensure that cybercriminals cannot easily evade prosecution by moving from one country to another. Going forward, more effective and concerted measures in law enforcement, public education, and capacity building are aspects that will help Indonesia become more resilient in the face of cybercrime. (Melati et al., 2021).

Conclusion

The conclusions of the research findings on Indonesia's criminal law reform in the face of cybercrime show that although there is a basic legal framework in the form of the ITE Law that covers various aspects of cybercrime, reforms are still needed to strengthen the legal system and its enforcement. The development of the ITE Law, sharpening definitions and boundaries of legal rules to avoid multiple interpretations, as well as alignment with human rights and civil liberties standards, are needed to create a safer and fairer digital environment. Greater legal clarity will reduce the potential for abuse of power and increase public and business confidence in Indonesia's cyber justice system.

In addition, the study also emphasised the need to improve human resources and technological infrastructure to support effective law enforcement against cybercrime. This includes investment in the training of law enforcement personnel, procurement of the latest technological equipment for investigations, and the

establishment of cooperation networks with international experts and institutions in the field of cybersecurity. Cross-border cooperation is essential due to the transnational nature of cybercrime. With more inclusive and modernised legal reforms, along with increased capacity in law enforcement, Indonesia can move towards a criminal justice system that is more efficient and responsive to cybercrime, thus protecting its citizens and infrastructure from digital threats.

Thus, Indonesia's criminal law reform in the face of cybercrime requires improvements in the ITE Law to ensure legal clarity, avoid multiple interpretations, and strengthen the protection of human rights and civil liberties. In addition, improvements in human resources and information technology are needed to increase the effectiveness of law enforcement. International cooperation is also critical to address the transnational nature of cybercrime and ensure Indonesia is able to address cybersecurity challenges more effectively.

References

Abdul, M., Ingabire, A., Lam, C., Bennett, B., & ... (2024). Indigenous food sovereignty assessment-A systematic literature review. *Nutrition & ...*, *Query date: 2024-05-10 07:14:07*. https://doi.org/10.1111/1747-0080.12813

Adhi, M., & Soponyono, E. (2021). Crime Combating Policy of Carding in Indonesia in the Political Perspective of Criminal Law. *Law Reform*, *Query date: 2024-05-14 19:37:38*. https://ejournal.undip.ac.id/index.php/lawreform/article/view/41736

Angga, A., Utomo, B., & Syam, F. (2023). The Role of Legal Politics in the Formulation of Law No. 1 Year 2023 on the Criminal Code. *AL-MANHAJ: Journal of ...*, *Query date: 2024-05-14 19:37:38*. https://ejournal.insuriponorogo.ac.id/index.php/almanhaj/article/view/3895

Anwar, M. (2023). The urgency of reforming regulations for money laundering in the digital era. *East Asian Journal of Multidisciplinary ...*, *Query date: 2024-05-14 19:37:38*. https://journal.formosapublisher.org/index.php/eajmr/article/view/5009

Azhari, M. (2024). Criminal Case Handling in Indonesia: Challenges, Reforms, and Future Directions. *... Restructuring and Transforming Law*, *Query date: 2024-05-14 19:37:38*. https://proceedings.ums.ac.id/index.php/icrtlaw/article/view/3624

Azizah, S., Asikin, Z., & Parman, L. (2021). Implementation of E-Commerce Crime Law Enforcement at the West Nusa Tenggara Regional Police. *International Journal of Multicultural and ...*, *Query date: 2024-05-14 19:37:38*. https://ijmmu.com/index.php/ijmmu/article/view/2273

Barlian, A., & Herista, A. (2020). Virtual Court as Alternative on the Future Criminal Justice System in Indonesia. *Proceedings of The International ...*, *Query date: 2024-05-14 19:37:38*. https://doi.org/10.4108/eai.26-9-2020.2302367

Budianto, E., & Wulandari, D. (2020). Critical study of criminal aspects of Law Number 8 of 1999 concerning consumer protection. *Journal of Law and Legal Reform*, *Query date: 2024-05-14 19:37:38*. https://journal.unnes.ac.id/sju/jllr/article/view/36623

Damayanti, D., & Ismowati, M. (2021). The Implementation Of The Cybercrime Prevention Policy At The Metro Jaya Police Station In Central Jakarta. *Proceedings Of The 1st International ...*, *Query date: 2024-05-14 19:37:38.* https://doi.org/10.4108/eai.17-7-2019.2302054

Darma, I. (2021). The Penal Policy Formulation in Cyberporn Crime Countermeasures. *Journal of Magister Hukum Udayana*, *Query date: 2024-05-14 19:37:38.* https://ojs.unud.ac.id/index.php/jmhu/article/download/59062/39151

Emaliawati, E. (2024). Defamation in the Digital Age: An Analysis of the Application of Restorative Justice under Indonesian Criminal Law. *Intellectual Law Review (ILRE)*, *Query date: 2024-05-14 19:37:38.* https://jurnal.ysci.or.id/ILRE/article/view/62

Fadhil, M. (2023). Criminal Law Reform in Indonesia: The Perspective on Freedom of Expression and Opinion. *Al-Jinayah: Journal of Islamic Criminal Law*, *Query date: 2024-05-14 19:37:38.* https://jurnalfsh.uinsby.ac.id/index.php/HPI/article/view/1871

Fitran, M., & Santiago, F. (2022). Digital Crime on Account of Defamation of the President of the Republic of Indonesia. *Proceedings of the First Multidiscipline International ...*, *Query date: 2024-05-14 19:37:38.* https://doi.org/10.4108/eai.30-10-2021.2315765

Hamanduna, A., & Widjanarko, P. (2023). Discourse network on the revision of Indonesian information and electronic transaction law. *Journal of Communication Studies*, *Query date: 2024-05-14 19:37:38.* https://ejournal.unitomo.ac.id/index.php/jsk/article/view/5496

Hartati, S., Karyono, H., & Sabowo, H. (2022). Implementation of The Law on Information and Electronic Transactions and Pancasila Law Enforcement Related to Cybercrimes in Indonesia. *International Journal of Educational ...*, *Query date: 2024-05-14 19:37:38.* https://www.ijersc.org/index.php/go/article/view/290

Imran, M. (2023). Cyber Criminology: An analysis of the Indonesian and the United States Police Perception. *International Journal of Cyber Criminology*, *Query date: 2024-05-14 19:37:38.* https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/224

Ishak, S., Malik, F., & Suwarti, S. (2023). Analysis of Imprisonment Implementation against the Perpetrators of the Cybercrimes. *Journal of Social Science*, *Query date: 2024-05-14 19:37:38.* https://www.jsss.co.id/index.php/jsss/article/view/538

Khatrine, F. (2024). Criminal Law Reform of the Existence of Article 378 of the Criminal Code in Land Cases: Case Study of Judgment No. 1154/Pid. B/2021/PN. JKT. SE. *Indonesian Journal of Social Science*, *Query date: 2024-05-14 19:37:38.* https://jiss.publikasiindonesia.id/index.php/jiss/article/view/1082

Koto, I. (2021). Cyber crime according to the ITE law. *International Journal Reglement &Society ...*, *Query date: 2024-05-14 19:37:38.* http://jurnal.bundamediagrup.co.id/index.php/ijrs/article/view/124

Lindsey, T., & Pausacker, H. (2020). Crime and punishment in Indonesia. *Crime and Punishment in Indonesia*, *Query date: 2024-05-14 19:37:38.* https://doi.org/10.4324/9780429455247-1

Listiyanto, E., & Arpangi, A. (2021). Implementation Effectiveness Of Police Role In Eradication Of Online Gaming Crime In Digital Era. *Law Development Journal*, *Query date: 2024-05-14 19:37:38.* https://jurnal.unissula.ac.id/index.php/ldj/article/view/16072

Mahardhika, V. (2021). An Electronic Court in the Perspective of Criminal Law Reform. *International Joint Conference on Arts and ...*, *Query date: 2024-05-14 19:37:38.* https://www.atlantis-press.com/proceedings/ijcah-21/125967462

Manullang, H., Habeahan, B., & Nduru, I. (2023). The Politics of Criminal Law in Tackling Crimes Under the Guise of Electronic Investment in Indonesia. *UNES Law Review*, *Query date: 2024-05-14 19:37:38.* https://review-unes.com/index.php/law/article/view/1189

Melati, D., Rosidah, N., & Siswanto, H. (2021). Implementation of Organised Cyber Crime Countermeasures Against National Investment. *JL Pol'y &Globalisation*, *Query date: 2024-05-14 19:37:38.* https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jawpglob115§ion=7

Nawawi, J., Darmawati, D., Tajuddin, M., & ... (2023). The Law Enforcement Related to Cyber Crime by Involving the Role of the Cyber Patrol Society in Achieving Justice. *Journal of IUS Studies ...*, *Query date: 2024-05-14 19:37:38.* https://jurnalius.ac.id/ojs/index.php/jurnalIUS/article/view/1289

Nesset, V., Vanderschantz, N., & ... (2024). Advocating for a more active role for the user in LIS participatory research: A scoping literature review. *Journal of ...*, *Query date: 2024-05-10 07:14:07.* https://doi.org/10.1108/JD-11-2022-0254

Nugraha, M. S., Liow, R., & Evly, F. (2021). The Identification of Online Strategy Learning Results While Students Learn from Home During the Disruption of the COVID-19 Pandemic in Indonesia. *Journal of Contemporary Issues in Business and Government*, *27*(2), Article 2.

Nurahman, D. (2020). Cybercrime Policies: Juridical Evidence and Law Enforcement Policies. *CCER*, *Query date: 2024-05-14 19:37:38.* https://doi.org/10.4108/eai.26-9-2020.2302579

Nurkholim, N. (2020). The Strength of Electronic Document Evidence in Crime based on Technology and Information (Cyber Crime). *Mantik Journal*, *Query date: 2024-05-14 19:37:38.* https://www.ejournal.iocscience.org/index.php/mantik/article/view/1485

Pansariadi, R., & Soekorini, N. (2023). Cyber Crime and its Law Enforcement. *Binamulia Hukum*, *Query date: 2024-05-14 19:37:38.* https://ejournal.hukumunkris.id/index.php/binamulia/article/view/605

Prasetyo, S., & Hidayah, N. (2020). Identity Theft and the Rules in Indonesia's Criminal Law. *... Conference on Law Reform ...*, *Query date: 2024-05-14 19:37:38.* https://www.atlantis-press.com/proceedings/inclar-19/125935422

Puspitosari, S. H. (2020). *Cybercrime in the field of Decency: Information Technology and Morality*. books.google.com. https://books.google.com/books?hl=en&lr=&id=c6j7DwAAQBAJ&oi=fnd&pg=PR5&dq=reform+indonesian+criminal+law+cyber+crime&ots=r0vC7HIHkm&sig=A3iR03BhtMUbe5_bUH9JpSFnnEA

Putri, A., Arum, Q., Sabena, T. D., & ... (2024). Criminal Law Policy in Tackling Fake News Crime. *... Transforming Law*, *Query date: 2024-05-14 19:37:38*. https://proceedings.ums.ac.id/index.php/icrtlaw/article/view/3629

Raharjo, A. (2021). Prevention of Cybercrime through the Development of Criminal Responsibility Principles for Internet Users. *Journal of Legal Dynamics*, *Query date: 2024-05-14 19:37:38*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4219956

Siregar, G., & Sinaga, S. (2021). The law globalisation in cybercrime prevention. *International Journal of Law...*, *Query date: 2024-05-14 19:37:38*. http://repository.darmaagung.ac.id/id/eprint/99/

Suhendi, D., & Asmadi, E. (2022). Cyber laws related to prevention of theft of information related to acquisition of land and infrastructure resources in Indonesia. *International Journal of Cyber ...*, *Query date: 2024-05-14 19:37:38*. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/35

Supeno, B., & Krismiyarsi, K. (2023). Criminal Politics Criminal Actions of Information and Electronic Transactions (Within the Framework of Criminal Law Reform). *International Conference on Law ...*, *Query date: 2024-05-14 19:37:38*. https://www.atlantis-press.com/proceedings/icleh-22/125985825

Suprapto, D., Faslukil, M., & Triyana, Y. (2023). Indonesia's Role in Preventing Transnational Cyber Pornography of Children in the Southeast Asian Region Viewed From a Political Law Approach. *... Journal of Social Science and Human ...*, *Query date: 2024-05-14 19:37:38*. https://ijsshr.in/v6i6/Doc/83.pdf

Takdir, M., & Fitriasih, S. (2023). Indonesia's Criminal Law Policy in Tackling Cyberbullying with a Restorative Justice Approach. *Legal Brief*, *Query date: 2024-05-14 19:37:38*. http://legal.isha.or.id/index.php/legal/article/view/733

Teixeira, J., & Carvalho, A. (2024). Corporate governance in SMEs: A systematic literature review and future research. *... : The International Journal of Business in ...*, *Query date: 2024-05-10 07:14:07*. https://doi.org/10.1108/CG-04-2023-0135

Trisiana, A., & Utami, R. (2022). Smart Mobile Civic" based on the Project Citizen Model as an Effort to Optimise Citizenship Learning in the Independent Campus Era. *Journal of Internet Services and Information ...*, *Query date: 2024-05-14 15:26:32*. https://jisis.org/wp-content/uploads/2023/01/I4.005.pdf

Wahyuningsih, S., Juita, S., Masdurohatun, A., & Iksan, M. (n.d.). Criminal Responsibility System Against Online Criminal Acts of Prostitution in Indonesia. *Academia.Edu*, *Query date: 2024-05-14 19:37:38*. https://www.academia.edu/download/102882696/6.pdf

Yuhernawa, Z., & Fakrulloh, Z. (2021). Juridical Analysis of Criminal Law Enforcement on the Criminal Acts of Online Business Fraud. *... 2021: Proceedings of the 1st ...*, *Query date: 2024-05-14 19:37:38*. https://doi.org/10.4108/eai.6-3-2021.2306888

YULIANTO, F., & SUGIRI, B. (2022). Electronic Criminal Trial Reform That Guarantees Due Process Of Law. *International Journal of ...*, *Query date: 2024-05-14 19:37:38*. https://www.journalkeberlanjutan.com/index.php/ijesss/article/view/273

Yusni, M., & Sigalingging, B. (2022). Encryption as The Legal Protection Against Cybercrimes Associated with Digital Land Certificates in Indonesia. *International*

Journal of Cyber..., *Query date: 2024-05-14 19:37:38.* https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/34

Zulhidayat, M. (2020). CYBERPORN ANALYSIS IN THE PERSPECTIVE OF THE IUS CONSTITUTUM IN INDONESIA. *JHR (Replik Law Journal)*, *Query date: 2024-05-14 19:37:38.* http://jurnal.umt.ac.id/index.php/replik/article/view/3018