JoLSIC
Journal of Law, Society, and Islamic Civilization
Editorial Office: Faculty of Law, Universitas Sebelas Maret, Surakarta, 57126, Indonesia.
Phone: +6271-646994
E-mail: JoLSIC@mail.uns.ac.id
Website : https://jurnal.uns.ac.id/JoLSIC/index

Cyber Crime in Renewing The ITE Law to Realize The Goals of Legal Justice

Adwi Mulyana Hadi

Faculty of Law, Sekolah Tinggi Hukum Bandung, Bandung, Indonesia.
**Corresponding author's e-mail: adwimulyanah@gmail.com*

Article

Keywords:

cybercrime, justice, perpetrators, protection, victims

Artikel History
Received: Mar 6, 2023;
Reviewed: Apr 20, 2024;
Accepted: Apr 21, 2024;
Published: Apr 30, 2024.

DOI:
10.20961/jolsic.v12i1.85197

Abstract

Cybercrime in Indonesia is currently regulated by the Electronic Information and Transactions (ITE) Law, but it is considered inadequate to accommodate the various developments of cybercrime, so that renewing the ITE Law is important. The renewal of the ITE Law is needed to provide legal certainty and adequate protection for the public, as well as to improve the effectiveness of law enforcement against cybercrime perpetrators. The purpose of this study is to evaluate the regulation of cybercrime in the ITE Law with a focus on justice and victim protection aspects as well as to identify matters that need to be regulated and refined in the renewal of the ITE Law related to cybercrime. This study uses a normative method with a statutory and conceptual approach, analyzing primary, secondary and tertiary legal materials related to cybercrime. Data were collected through literature study then analyzed descriptively qualitatively to formulate problem solving recommendations based on the results of the analysis. The results of the study illustrate that the regulation of cybercrime in the current ITE Law is still considered weak in providing justice and protection for victims. This can be seen from the limited definition of cybercrime, unclear elements of criminal acts, weak victim protection, as well as excessive and disproportionate criminal provisions. Therefore, renewing the ITE Law is necessary to expand the definition of cybercrime, refine the formulation of criminal acts, increase victim protection, adjust criminal sanctions, and regulate recovery systems for aggrieved parties in order to achieve better justice and legal certainty.

INTRODUCTION

Cybercrime or cybercrime has become an important issue in law enforcement in Indonesia in recent years. Criminal acts in cyberspace or cybercrime are a form of crime that is increasingly common in the current digital era (Iftitah, 2023b). The development of technology and the internet has given birth to a new dimension in people's lives which allows criminals to take advantage of gaps in cyberspace to commit criminal acts (Sari, 2022). The rise in cases of cyber crime such as online fraud, theft of personal data, defamation, and so on is a challenge for the government and law enforcement officials.

Currently, Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) is the main legal basis for dealing with criminal acts in cyberspace in Indonesia. However, the ITE Law is considered not yet fully able to accommodate the increasingly growing variety of forms of cybercrime. The loopholes contained in the ITE Law open up the potential for abuse of the law, excessive punishment, and injustice towards human rights.(Setiawan & Arista, 2013). Therefore, there is an urgent need to reform the ITE Law to adapt to technological developments and overcome existing weaknesses, so as to provide better protection for society, ensure justice, and avoid potential abuse of the law.

One of the main objectives of the revision of the ITE Law is to further strengthen law enforcement efforts against cyber crimes. It is hoped that this revision will create legal instruments that are more effective and able to keep up with current developments, so that they can have a deterrent effect on cybercriminals. Of course, this revision is also aimed at realizing the most basic legal goal, namely achieving legal justice. However, the process of revising the ITE Law itself is not easy, there are various obstacles that must be faced. Starting from differences of opinion between the government and the DPR, to the balance between aspects of legal certainty and protection of freedom of opinion in cyberspace (Perkasa & Pakpahan, 2023). Therefore, an in-depth scientific study is needed regarding what strategic steps need to be taken in revising the ITE Law in order to achieve legal justice for society.

The expansion and revision of several articles in the ITE Law is a major concern in the context of accommodating the development of criminal acts in cyberspace. One of the articles in the spotlight is Article 27 paragraph (3) which regulates defamation. Evaluation shows that the formulation of this article is too broad, creates legal uncertainty, and has the potential to be misused by certain parties for criminalization purposes which can hamper freedom of expression (Budiman et al., 2021). Therefore, revisions to Article 27 paragraph (3) need to consider clearer explanations, stricter limitations, and protection of the right to freedom of expression in order to create regulations that are balanced, effective, and do not harm individual rights.

Current cyber crimes include various serious threats such as hacking of data and information (hacking), fraud in electronic transactions (phishing), defamation, and the spread of fake news (hoaxes) in cyberspace, as well as the use of fake accounts and other people's identities without agreement. Data released by the National Police shows that during 2021, there were more than 6,000 cybercrime cases that were successfully handled by the authorities, especially in the field of online fraud (Hapsari & Pambayun, 2023). This high number of cases creates a big opportunity

for similar crimes to continue to grow. This phenomenon highlights the urgency of improvements in the regulation of cyber crime, as discussed previously, to overcome increasingly complex challenges and protect society from ever-increasing cyber threats.

The current massive number of cybercrime cases can be understood as the impact of the lack of special regulations regarding cybercrime in the applicable ITE Law. The ITE Law tends to be general in nature, not yet including provisions that specifically address various new types of cybercrimes that continue to develop. Apart from that, the law's inadequacy in protecting and providing justice to victims of cybercrimes is a significant problem. This can be seen from the continued rise in defamation cases in cyberspace without adequate legal protection for victims. Therefore, the criminalization of cyber crimes needs to be adapted to current developments in order to create justice and proportional benefits for the parties involved. The formulation of new cyber offenses in the renewal of the ITE Law is also needed to provide legal certainty and adequate protection for the community. Apart from that, criminalization must also be oriented towards the goal of restorative and reconciliatory punishment which prioritizes recovery for the parties, not just retaliation (Habibi & Liviani, 2020).

Apart from weaknesses in regulating cyber crimes, the ITE Law also faces challenges in regulating the removal of content on digital platforms which are considered unclear. Lack of adequate safe harbor provisions can increase the risk of punishment for electronic system operators such as Facebook and Twitter due to illegal content uploaded by users. As a result, this risk could lead to restrictions on freedom of expression on these platforms (Frensh, 2022). Therefore, revisions are needed in the ITE Law that can clarify the responsibilities of organizers regarding the removal of illegal content, so as to create a clearer legal framework and provide more effective protection without sacrificing freedom of expression in the digital realm.

Furthermore, increasing the threat of criminal sanctions in the ITE Law is also one of the options being considered to eradicate cyber crime. Currently, the criminal sanctions in the ITE Law are considered too low to provide a deterrent effect for cybercriminals. The severity of the threat of punishment is important, but it also needs to be supported by considerations of justice. Therefore, the government and stakeholders must look for the best formulation regarding increasing sanctions, while still prioritizing the principle of proportionality in criminal law (Luthfiandari, 2023). From the background of the problems above, it is necessary to reform the ITE Law in a more comprehensive manner so that it is able to tackle various forms of cyber crime which are increasingly diverse and developing. This reform is important to ensure the realization of a sense of justice and legal certainty as well as adequate protection for the community, especially victims of cyber crime.

Some of the objectives of updating the ITE Law include (Hartanto, 2021):

a. Providing legal certainty and adequate protection for victims of cyber crime
b. Refining a more comprehensive formulation of cyber crime according to the developing forms and modes of crime
c. Affirming the responsibilities and obligations of related parties, especially digital platform managers, so that they can contribute to efforts to prevent and prosecute cyber crimes

d. Organize efforts for reconciliation and restoration in a fair manner for parties who have suffered losses due to cyber crimes
e. Increasing the effectiveness of law enforcement against perpetrators of cyber crimes through clear and measurable regulations

In this regard, comprehensive scientific research is important to provide targeted recommendations in the process of revising the ITE Law. It is hoped that these studies can support the formation of regulations that effectively deal with crime in cyberspace, while guaranteeing freedom of opinion and the digital rights of netizens in accordance with the constitution. The problem formulation in this research is as follows:

a. How is the regulation of cyber crimes in the ITE Law currently viewed from the aspect of justice and protection for cybercrime victims?
b. What needs to be regulated and refined in the renewal of the ITE Law regarding cyber crimes to better guarantee the realization of legal justice and protection for victims?

RESEARCH METHODS

This research uses normative legal research methods, namely research on legal principles and rules contained in statutory regulations related to research problems (Iftitah, 2023a). This research uses a legislative approach, by examining various regulations relating to cyber crime in Indonesia. This research also uses a conceptual approach by examining various concepts and theories in the field of law as a basis for analysis.

This research uses primary legal materials, namely laws and regulations related to cyber crimes and legal justice such as the ITE Law, Criminal Code, and Cyber Crime Bill. Secondary legal materials are obtained from legal textbooks, research journals, and expert opinions. Tertiary legal materials are sourced from legal dictionaries and official government websites. The data used as research material was collected through literature study to obtain primary, secondary and tertiary legal materials. Data was also collected through content analysis of various research-related documents (Hakim, R., & Mezak, 2013).

Data analysis uses descriptive analytical techniques. The data obtained was studied thoroughly and then categorized and analyzed based on legal materials to conclude the dynamics and problems of regulating cyber crimes in the renewal of the ITE Law in order to realize the goals of legal justice. The data was analyzed qualitatively in order to obtain an objective picture regarding the problems studied. Problem solving recommendations are formulated based on the results of the data analysis.

ANALYSIS AND DISCUSSION

1. Regulation of Cyber Crime in the ITE Law is Currently Viewed from the Aspect of Justice and Protection of Cybercrime Victims

Regulations regarding cyber crime in Indonesia are currently regulated in Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE). However, the regulations in the ITE Law are considered to be still inadequate in providing justice and protection for victims of cybercrime. Some of the weaknesses found include the limited

definition of cyber crime, unclear elements of certain criminal acts, and weak victim protection.

Articles 27 to 37 of the ITE Law provide the legal basis for various criminal acts in the field of information technology, however, these regulations are still general in nature and unable to specifically address the development of cybercrime which continues to grow. Real examples can be seen in types of crime such as phishing, carding, cybersquatting, and so on, which are currently on the rise, but are not yet explicitly regulated in the ITE Law. Apart from that, the formulation of the articles in the ITE Law still has multiple interpretations, creating legal uncertainty and leaving room for criminals in cyberspace (Agustian & Manik, 2021). As a result, law enforcement becomes hampered, and the gaps open to cybercriminals widen.

Cybercrime regulations in the ITE Law currently tend to focus more on criminalizing actions that have the potential to harm many people, such as illegal access, phishing and the distribution of illegal content. However, the main shortcoming lies in the lack of explicit provisions governing the form of legal protection and compensation for individual victims resulting from cybercrime. Many cases of cybercrime, such as theft of personal data, defamation, extortion and online threats, do not receive adequate protection. Apart from that, the criminal provisions in the ITE Law do not fully reflect justice, especially in relation to punishments that are considered excessive or overcriminalization (Muhammad & Harefa, 2023).

Many articles in the ITE Law threaten imprisonment and large fines, often reaching 6 years in prison and more than IDR 1 billion for ordinary crimes. This is certainly disproportionate and has the potential to harm justice. In fact, criminal law must be enforced as a last resort (ultimum remedium) by considering the impacts and losses caused. A restorative justice approach that provides compensation and rehabilitation for victims also needs to be prioritized, not just the punishment of perpetrators (Hartono et al., 2018). Thus, the application of criminal sanctions needs to be adjusted to balance the interests of protecting victims and punishing perpetrators without being excessive.

New cyber offenses such as illegal access, phishing, spamming and others have also not been accommodated adequately. As a result, law enforcement in cybercrime cases is not optimal and has received a lot of criticism from the public. An example of this is the widespread incidence of doxing, namely the distribution of other people's information and personal data on the internet without consent (Sari, 2022). Based on Article 27 paragraph (1) of the ITE Law, this action is punishable by imprisonment for a maximum of 6 years and/or a fine of IDR 1 billion. However, this law does not regulate a compensation mechanism for victims for loss of confidentiality of their personal data due to doxing. In fact, the impact of doxing can be very detrimental and tarnish the victim's good name.

Then there is another problem, although the ITE Law regulates the removal of illegal content such as defamation, there is no article that explicitly requires perpetrators to apologize and pay compensation to victims resulting from such content. On the contrary, there is actually a criminal threat for the victim if they participate in distributing evidence of the defamatory

act (Ali, 2016). This condition clearly does not reflect justice and tends to harm cybercrime victims. The victim should have the right to receive recovery for the material and immaterial losses suffered as a form of accountability for the perpetrator. Without clear compensation and restitution obligations, the perpetrator can escape responsibility by simply serving a prison sentence or a fine.

Apart from the material criminal law side, the ITE Law is also considered weak in providing protection for victims of cyber crime. The absence of regulations that require digital platforms and electronic system providers to delete information that invades privacy and harms someone is a loophole that has the potential to harm victims. The absence of civil regulations that provide compensation or compensation for cybercrime victims also has the potential to not provide a sense of justice for the injured party (Wahyudi, 2013). Some examples of cases that show injustice and the lack of protection for victims in the current ITE Law include the rise in cases of defamation, the use of fake identities in cyberspace, the distribution of other people's photos and information without permission, as well as cases of cyberbullying which have resulted in acts of violence even up to suicide.

In these cases, the ITE Law is considered "one-sided" and tends to protect the perpetrators, while victims whose personal rights are violated do not receive adequate justice and protection. For example, for defamation, it is the reporter who often faces the law as a result of reporting actions that are detrimental to him. Meanwhile the perpetrator walked free without any punishment. Therefore, updating the ITE Law is necessary to further strengthen protection for cybercrime victims (Yanto, 2020). For example, by adding an article related to the victim's right to compensation for losses and restoration of reputation due to cyber criminal acts that harm them. Apart from that, it would be good to add provisions that require perpetrators, apart from imprisonment or fines, to provide restitution and take certain actions such as an apology to recover the victim's losses.

Thus, law enforcement against cyber crimes is not only about punishing the perpetrators, but also providing justice and reparation for the affected victims (Adwi Mulyana Hadi, Anik Iftitah, 2023). This is important to ensure the fulfillment of victims' human rights and restore public trust in law enforcement in the cyber realm. Based on this description, it appears that the ITE Law is still weak in providing legal protection and justice for the community regarding cybercrime. Therefore, it is necessary to improve the ITE Law in a more comprehensive manner so that it is in line with the principles of justice and able to accommodate various cyber criminal acts that continue to develop. This update is important to provide certainty, protection and legal justice for the community, both victims and perpetrators of cybercrime (Iftitah, 2023c).

Criminal law should be used as a last resort, prioritizing the principle of ultimum remedium, where law enforcement must be considered carefully, taking into account the impacts and losses that may arise. Apart from that, the restorative justice approach, which focuses on providing compensation and rehabilitation for victims, must receive primary attention, not just focus on punishing the perpetrator. The importance of harmonizing the

application of criminal sanctions to achieve a balance between protecting victims and punishing perpetrators without causing excess or disproportionality is essential in this context. With this approach, it is hoped that the objectives of criminal law, which aim to protect the interests of individuals and society fairly, can be realized, creating a legal system that is more holistic and supports true justice (Iftitah, 2017).

2. Things that need to be regulated and perfected in the renewal of the ITE Law regarding cyber crimes to better ensure the realization of legal justice and protection for victims

Cybercrime or cybercrime is a form of crime in cyberspace that is increasingly common in line with the rapid development of information and communication technology in recent years. Cybercrime itself can be defined as an illegal act that uses the internet and computer networks to harm other parties. Some examples of cyber crimes include theft of personal data and information (hacking), online fraud (phishing), website hacking (defacing), distribution of malware, and so on. The rise in cybercrime cases certainly poses a serious threat to security and public order in the digital era. Many of the regulations regarding cyber crimes in the ITE Law are still general in nature, unable to accommodate the various modus operandi of cyber crimes that continue to develop. Apart from that, the ITE Law also does not provide legal certainty and adequate protection for the public and victims of cybercrime.

One of the main legal instruments that regulates cybercrime in Indonesia today is Law Number 11 of 2008 concerning Electronic Information and Transactions or better known as the ITE Law. However, the ITE Law in the current context is considered inadequate and needs to be refined in order to deal with criminal acts in cyberspace which continue to develop rapidly in various forms of modus operandi. Some of the weaknesses of the current ITE Law include the limited definition of cyber crime, the formulation of articles that have multiple interpretations, the unclear elements of proof of a cyber crime, and the lack of optimal protection for cybercrime victims. This condition has the potential to hamper effective law enforcement processes in eradicating crime in cyberspace. Therefore, it is very important to update or revise the ITE Law so that regulations in this field can keep up with current developments and be able to deal with cyber crimes which are increasingly sophisticated in their methods. Therefore, it is deemed necessary to immediately reform the ITE Law regarding cybercrime regulations. This update is expected to clarify various types of cyber crime and their elements, provide better legal certainty, and increase protection for the public and victims of cyber crime. It is also hoped that the reform will be able to support effective law enforcement against cybercrime perpetrators (Sari, 2022). In order to realize legal justice and protection for victims of cyber crime, there are several things that need to be further regulated and refined in the renewal of the ITE Law regarding cyber crimes, including:

To increase the effectiveness of law enforcement against cybercrime, the first step that needs to be taken is to expand the definition and regulation of types of cybercrime in more detail and comprehensively in accordance with current modus operandi developments. This includes types of crime such as phishing, skimming, cyberbullying, doxing, carding, malware

injection, database hacking, and so on (Habibi & Liviani, 2020). By detailing this definition, each type of cybercrime can be handled specifically according to its characteristics and impact, allowing law enforcement officials to be more efficient in investigation and prosecution. This clear formulation can also be the basis for updating the ITE Law to accommodate the ever-growing dynamics of cyberspace, so that legal policies can remain relevant and adaptive to new challenges in the realm of cyber crime.

Second, improvements are needed in the formulation of the elements of criminal acts in the ITE Law so that they do not have multiple interpretations. The main aim is to ensure legal certainty and prevent potential misuse of articles, so that justice can be realized. Currently, many articles in the ITE Law threaten criminal penalties with a level of objection that is not in line with the actual level of loss and impact caused. It is important to apply the principle of ultimum remedium in criminal law to ensure that the punishment imposed is truly effective in protecting the interests of society and victims (Malunsenge et al., 2022). Therefore, the elements of criminal acts, such as "electronic information and/or electronic documents," need to be formulated more clearly and measurably so as not to leave room for excessive interpretation.

Third, it is necessary to increase protection for victims of cybercrime, both individuals and corporations. This is important to restore the rights of cybercrime victims so that restorative justice can be enforced. Currently there are no special regulations that provide legal clarity regarding victims' rights and compensation procedures for them. With this arrangement, it is hoped that cybercrime victims can obtain complete justice. For example, by providing clearer civil lawsuit rights and compensation for victims. Then regulates the perpetrator's obligation to carry out rehabilitation and repair the reputation of victims due to defamation in cyberspace. It is also necessary to regulate administrative sanctions and fines for digital platform operators who are negligent in protecting users from illegal content and crime (Flora et al., 2023).

In the context of adjusting regulations related to cyber crime, the fourth aspect emphasizes the need to adjust criminal threats proportional to the level of harm caused. This aims to ensure that the punishment imposed is in line with the principles of justice. For example, providing leniency in criminal sanctions for cybercrime perpetrators who commit acts for the first time with small losses could be a fairer approach. On the other hand, tightening criminal sanctions need to be applied to corporations or internet platform operators who are negligent in their role in helping prevent cyber crime. The importance of the principle of ultimum remedium also needs to be emphasized, ensuring that punishment is the final step after other efforts have been carried out (Jainah, 2018).

Fifth, the importance of specifically regulating the recovery and restoration system in the context of cyber crimes is a crucial aspect in creating justice for the injured parties. In this case, it is necessary to consider returning financial losses to victims, restoring online reputation, as well as providing psychological counseling for those who are victims of fraud. This restorative justice approach not only ensures the punishment of the perpetrator, but also seeks to restore balance and trust between the parties involved. By detailing this recovery and restoration

system, it is hoped that the rehabilitative and restorative effects can be felt concretely by victims, helping them recover from the impacts of cyber crimes, as well as encouraging the creation of a fairer and more just legal environment (Ediyanto, 2023).

Sixth, in the context of increasing the effectiveness of prosecuting cybercrime, serious efforts are needed to increase the professionalism and authority of law enforcement officials. Steps involving cooperation between law enforcement agencies, appropriate transfer of competence, and provision of adequate facilities for investigators and prosecutors will be the key to success. This arrangement aims to ensure that law enforcement officials have sufficient capability and knowledge to investigate and handle cyber crimes efficiently. Without increased professionalism and clear authority, legal regulations related to cybercrime will only remain legal norms on paper that are unable to provide optimal results in fighting increasingly complex and rapidly developing cyber threats (Sriwidodo, 2020).

Seventh, it is necessary to regulate obligations for parties involved in information technology services, such as electronic system operators and internet service providers, to play an active role in preventing the occurrence of cybercrime, so that justice can be upheld comprehensively. These obligations include concrete actions such as blocking illegal content and reporting cybercrime to law enforcement officials. By involving various elements, it is hoped that efforts to suppress cyber crime can reach an optimal level, strengthening synergy between the private sector and the authorities in maintaining cyber integrity and security (Kakoe, 2019).

Eighth, the need to set up a clear mechanism for the removal of illegal content on the internet by electronic system operators is a critical aspect in the context of digital security. Currently, the existence of standard procedures for responding to content that violates the law, such as hate speech or false information/hoaxes, has not yet been realized. This mechanism for removing illegal content has great significance in protecting victims and preventing wider impacts on society. With regulations governing the process of removing illegal content, a clear and responsive framework will be created, enabling quick action to address potential dangers and violations of the law in cyberspace (Rahmawati et al., 2022).

Tenth, the importance of organizing international cooperation in investigating and prosecuting transnational cybercrime perpetrators becomes relevant in the context of increasing cybercrime cases involving perpetrators and victims from various countries. Effective cooperation between law enforcers in various countries is the key to overcoming the challenges faced by legal authorities in dealing with transnational cybercrime. With a good cooperative framework in place, law enforcement can pursue and punish cybercriminals, even if they operate outside national jurisdiction (Hapsari & Pambayun, 2023).

These are several important things that need to be regulated and refined in the renewal of the ITE Law regarding cyber crimes in order to achieve justice and protection for cybercrime victims. Comprehensive arrangements involving all stakeholders and in accordance with the latest technological developments and modus operandi are very urgent to ensure optimal law

enforcement in cyberspace. In this way, the interests of society and victims of cybercrime can be protected fairly in accordance with the objectives of the law.

CONCLUSION

The regulation of cyber crimes in the ITE Law is currently considered inadequate and has several weaknesses in terms of fulfilling justice and protecting cybercrime victims. Some of the weaknesses found include the limited definition of cyber crime, unclear elements of certain criminal acts, and weak victim protection. Apart from that, the punishment in the ITE Law is currently considered too heavy and disproportionate, so it is contrary to the principle of ultimum remedium in criminal law. It is considered that the ITE Law still does not provide justice and adequate legal protection for cybercrime victims. The absence of regulations that require perpetrators to provide compensation and apologies to victims is one of the weaknesses that makes it difficult for victims to obtain recovery. Things that need to be regulated and perfected in the renewal of the ITE Law related to cyber crimes in order to guarantee justice and protection of victims in general include: expanding the definition and regulation of types of cybercrime, refining the formulation of criminal acts so that there are no multiple interpretations, increasing victim protection through granting rights. prosecution and compensation, adjusting criminal threats to be more proportional, setting up a recovery and restoration system for injured parties, increasing the professionalism of law enforcement officials, regulating the obligations of parties regarding IT services, as well as international cooperation in prosecuting perpetrators of cross-border cybercrime.

Based on the research results, comprehensive reform is urgently needed to improve justice and protection for cybercrime victims. Improvements can be started by expanding the definition of cybercrime and refining the formulation of criminal acts so that they cannot be interpreted in multiple interpretations, as well as adjusting criminal threats to be more proportional. It is also important to increase the protection of victims by providing the right to sue and compensate, as well as setting up an effective recovery and restoration system. In addition, it is necessary to increase the professionalism of law enforcement officials, obligations for parties related to IT services, and international cooperation to take action against perpetrators of cross-border cybercrime. These steps will help create more balanced and effective regulations in addressing cybercrime, while still ensuring the rights and protection of victims.

REFERENCES

Adwi Mulyana Hadi, Anik Iftitah, and S. A. (2023). Restorative Justice Through Strengthening Community Legal Culture in Indonesia: Challenges and Opportunity. Mulawarman Law Review, 8(1), 32-44.

Agustian, R. A., & Manik, J. D. N. (2021). Tindak Pidana Informasi Elektronik dalam Kerangka Hukum Positif. PROGRESIF: Jurnal Hukum, 16(1), 92–111.

Ali, M. (2016). Pencemaran Nama Baik Melalui Sarana Informasi dan Transaksi Elektronik (Kajian Putusan MK No. 2/PUU-VII/2009). Jurnal Konstitusi, 7(6), 119-146.

Budiman, A. A., Maya, G. A. K. S., Rahmawati, M., & Abidin, Z. (2021). Mengatur Ulang Kebijakan Tindak Pidana di Ruang Siber Studi tentang Penerapan UU ITE di Indonesia. Institute for Criminal Justice Reform (ICJR).

Ediyanto, H. (2023). Rekonstruksi Regulasi Penghentian Penuntutan dalam Penegakan Hukum Oleh Kejaksaan Berbasis Nilai Keadilan Restoratif. Desertasi Program Doktoral, Universitas Islam Sultan Agung.

Flora, H. S., Sitanggang, T., Simarmata, B., & Karina, I. (2023). Keadilan Restoratif dalam Melindungi Hak Korban Tindak Pidana Cyber: Manifestasi dan Implementasi. Jurnal Ius Constituendum, 8(2), 169-184.

Frensh, W. (2022). Kelemahan Pelaksanaan Kebijakan Kriminal terhadap Cyber Bullying Anak di Indonesia. Indonesia Criminal Law Review, 1(2), 87-99.

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam, 23(2), 400–426.

Hakim, R., & Mezak, M. H. (2013). Jenis, Metode, dan Pendekatan dalam Penelitian Hukum. Ltiw Review. Law Review: Fakultas Hukum Universiius Pelita Harapan, 5(3), 85-97.

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman Cybercrime di Indonesia: Sebuah Tinjauan Pustaka Sistematis. Jurnal Konstituen, 5(1), 1–17.

Hartanto. (2021). Perlindungan Hukum Pengguna Teknologi Informatika Sebagai Korban dari Pelaku Cyber Crime Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Jurnal Hermeneutika, 5(2), 196-216.

Hartono, B., Jainah, Z. O., & Seftiniara, I. N. (2018). Kapita Selekta Tindak Pidana Ekonomi. Bandar Lampung: CV. Anugrah Utama Raharja.

Iftitah, A. (2017). Pancasila Versus Globalisasi: Antara Konfrontasi dan Harmonisasi? dalam Al Khanif dkk, Pancasila dalam Pusaran Globalisasi. Yogyakarta: LkiS.

Iftitah, A. (2023). Sejarah Perkembangan Hukum. In Pengantar Ilmu Hukum (Februari). Banten: Sada Kurnia Pustaka.

Iftitah, A. (Ed.). (2023). Metode Penelitian Hukum (Mei 2023). Banten: Sada Kurnia Pustaka.

Iftitah, A. (Ed.). (2023). Perkembangan Hukum Pidana di Indonesia. Banten: Sada Kurnia Pustaka.

Jainah, Z. O. (2018). Kapita Selekta Hukum Pidana. Tangerang: Tira Smart.

Kakoe, S. (2019). Perlindungan Hukum Korban Penipuan Transaksi Jual Beli Online Melalui Ganti Rugi Sebagai Pidana Tambahan dalam Undang-Undang Informasi dan Transaksi Elektronik. Tesis Program Magister Ilmu Hukum, Universitas Brawijaya.

Luthfiandari, R. (2023). Penegakan Hukum Terhadap Tindak Pidana Penipuan Investasi Bodong Berbasis Arisan Online (Studi Kasus di Kepolisian Resor Bojonegoro). Skripsi Program Sarjana Hukum Pidana Islam Fakultas Syariah dan Hukum, UIN Sunan Ampel.

Malunsenge, L. M., Massie, C. D., & Rorie, R. E. (2022). Penegakan Hukum terhadap Pelaku dan Korban Tindak Pidana Cyber Crime Berbentuk Phising di Indonesia. Lex Crimen, 11(3), 14-24.

Muhammad, F. E., & Harefa, B. (2023). Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web. Jurnal USM Law Review, 6(1), 226-241.

Perkasa, A., & Pakpahan, K. (2023). Kebijakan Penegak Hukum dalam Penanggulangan Tindak Pidana Perjudian Melalui Media Elektronik di Indonesia. SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan, 2(7), 2067-2084.

Rahmawati, M., Saputro, A. A., Marbun, A. N., Wicaksana, D. A., Napitupulu, E. A. T., Ginting, G. L. A., Tedjaseputra, J. A., Farihah, L., Siagian, M. N., Sati, N. I., & Pamintori, R. T.

(2022). Peluang dan Tantangan Penerapan Restorative Justice dalam Sistem Peradilan Pidana di Indonesia. Jakarta Selatan: Institute for Criminal Justice Reform.
Sari, U. I. P. (2022). Kebijakan Penegakan Hukum dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police di Indonesia. Jurnal Studia Legalia, 2(01), 58–77.
Setiawan, R., & Arista, M. O. (2013). Efektivitas Undang-Undang Informasi dan Transaksi Elektronik di Indonesia dalam Aspek Hukum Pidana. Recidive, 2(2), 139-146.
Sriwidodo, J. (2020). Perkembangan Sistem Peradilan Pidana di Indonesia. Yogyakarta: In Kepel Press.
Wahyudi, D. (2013). Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime Di Indonesia. Jurnal Ilmu Hukum Jambi, 4(1), 98-113.
Yanto, O. (2020). Negara Hukum: Kepastian, Keadilan dan Kemanfaatan Hukum (Dalam Sistem Peradilan Pidana Indonesia. Bandung: Pustaka Reka Cipta.