cek

by Ruang Buku

Submission date: 13-Feb-2024 08:44AM (UTC+0400)
Submission ID: 2293554900
File name: 8288-24631-3-ED.doc (255.5K)
Word count: 8462
Character count: 48940

Legal Protection For Victims Of Cybercrime As A Form Of Transnational Crime

Abstract

In addition to creating laws and regulations that safeguard victims of phishing, the goal of this research is to establish legal protection for victims of cybercrime, a form of transnational crime. This study employs a normative juridical research methodology that blends statutory and conceptual frameworks. The following are the results of the research: 1) Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions and Law Number 27 of 2022 concerning Personal Data Protection are examples of previous legislative regulations that regulate protections for victims of cross-border information crimes and electronic transactions. 2) Cybercrime victims' legal protection as a form of transnational crime. Essentially, two methods are available for use: 1) the procedural rights model, in which the victim has the right to attend all court proceedings and takes a more active role in the prosecution; 2) The service model, according to which victims are seen as individuals who require assistance from law enforcement in order to feel as though their rights are upheld in a just setting. Every step of the investigation, trial, and post-trial phases of the process needs to include virtual and in-person support for victims of cybercrime.

Keywords: *Legal Protection, Victims, Cyber, Transnational Crime*

1. INTRODUCTION

In order to realize a better economic life, technological advancement in the national economy is enhanced to achieve the welfare of the people.[1] The advent of the modern globalization era has made it impossible to separate technological assistance from any kind of community activity. The financial industry is starting to integrate with electronic system platforms in a similar manner. The advancement of technology and the internet significantly affects human existence. Since technological advancement will always follow scientific advancement, it is something we cannot stop in this lifetime. In actuality, technology is a tool or an extension of human capabilities. It now functions as a force that genuinely restrains our own actions and way of life. Due to its immense power, rapid advancement, and reinforcement by robust social structures, technology has taken on a directorship over human existence.

Cybercrime problems are crimes that occur in the cyberworld and can only be committed with the use of cybertechnology. Cybercrime issues have always been an interesting problem for several reasons, among others; because the problem is still relatively new, related to technology that only some people are able to do, the limited reach of the law to anticipate and so on.

The negative effects of technological advancements give rise to crimes in cyberspace. Crimes of all kinds have an impact on users' legal protection, which is crucial given that every person has a right to be protected in accordance with his or her inherent dignity. Providing legal guarantees and practical measures to shield the community from

---

[1] Raden Ani Eko Wahyuni And Darminto Hartono, "Implementation Of Legal Protection By The Government In Order To Empowerment Of Micro Small Medium Enterprise To Realize The Justice Economy (Research Study: The Office Of Cooperative And Micro Small And Medium Enterprise Province Of Central Java)," *Diponegoro Law Review* 4, No. 1 (2019): 388, Https://Doi.Org/10.14710/Dilrev.4.1.2019.388-396.

all types of crime or other deviant acts that the community may encounter both in the real world and in cyberspace is one way that the state protects its citizens.[2]

According to the constitution, Indonesia is a state of law. As such, the state has a duty to defend its citizens against any action that could endanger them, let alone actions that could jeopardize the stability of the country or state. For example, crimes committed online, also known as cybercrime. The sophistication of technology that is abused by careless people for their own gain has made it difficult for developing countries to take action against computer criminals, especially the police. In addition to the need for a set of rules governing the misuse of this information, human resources, supporting facilities, and infrastructure are also needed. This crime that knows no bounds to space or time has recently experienced rapid development.[3]

Crimes caused by the internet can also have a transnational dimension, commonly referred to as transnational crimes. Crimes are crimes that essentially have a national dimension but have transnational or cross-border characteristics. The locus delicti of transnational crimes in reality is still within the territorial boundaries of a country, but in practice transnational crimes involve the affairs of other countries, so it is as if there are two or more countries that have an interest in the crime. So the real core of transnational crime is that it has a national dimension, but due to the interconnectedness with the interests of other countries, it appears to be transnational in nature.[4]

One of the crimes related to the internet and has a transnational dimension is a crime that we can call cybercrime or crime through the internet network. According to the Ministry of Foreign Affairs of the Republic of Indonesia, cybercrime is included in the category of transnational crimes, considering that one of the special characteristics of cybercrime is that this crime is committed online and is often not clearly linked to any geographical location, so it often transcends the boundaries of other countries. And one of the characteristics of transnational crime is that it is committed beyond national borders, so this cybercrime has fulfilled one of the requirements to be called a part of transnational crime.

The legal protection for victims of cybercrime as a form of transnational crime is a complex and challenging issue. The global nature of cybercrime presents significant difficulties for law enforcement and legal protection. The challenges arise from the fact that cybercrime transcends national borders, making it difficult to apply traditional legal frameworks. The existing legal protection for cybercrime victims, such as Law Number 19 of 2016, may not provide significant relief to the victims.[5] This is compounded by the

---

[2] Endang Prastini, "Kebijakan Kriminal Pemerintah Terhadap Kejahatan Dunia Maya (Cyber Crime) Di Indonesia," *Jurnal Surya Kencana Dua*, 2018.
[3] Prastini.
[4] Danel Aditia Situngkir, "Asas Legalitas Dalam Hukum Pidana Nasional Dan Hukum Pidana Internasional," *Soumatera Law Review*, 2018.
[5] Angkasa Angkasa And Rili Windiasih, "Cybercrime Di Era Industri 4.0 Dan Masyarakat 5.0 Dalam Perspektif Viktimologi," *Journal Justiciabelen (Jj)* 2, No. 2 (2022): 104, Https://Doi.Org/10.35194/Jj.V2i2.2113.

underreporting of cybercrimes to the police, as most victims do not report these crimes.[6] Furthermore, the lack of comprehensive protection for victims is evident in the psychological and financial impact of cybercrime victimization, where victims often face blame from their social surroundings and legal institutions.[7] In the context of transnational crime, cybercrime is a significant concern due to its global nature and the challenges it poses for law enforcement and legal protection. The term "transnational crime" refers to crimes that have a link between the jurisdictions of two or more countries, and cybercrime fits this description due to its cross-border nature. However, the current legal categories may not fully reflect the linkages between cyber-dependent and cyber-enabled crime, highlighting the need for a more comprehensive legal framework to address transnational cybercrimes.[8]

In addressing the legal protection for victims of cybercrime as a form of transnational crime, it is essential to consider the applicability of routine activity theory in understanding cybercrimes and increasing awareness among citizens about their online activities and the types of protection available to prevent victimization.[9] Additionally, the criminology and victimology perspectives can provide insights into the motives, factors, and responses to cybercrimes, as well as the role of victims in addressing cybercrime.[10] Overall, the legal protection for victims of cybercrime as a form of transnational crime requires a multifaceted approach that considers the global nature of cybercrimes, the challenges in law enforcement, and the need for comprehensive legal frameworks to address transnational cybercrimes.

For the best possible development, laws that specifically forbid computer crime and offer legal protections against the use of media, information technology, and communication are required in light of the aforementioned circumstances. To handle the various issues listed above, the government passed Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). Furthermore, as stipulated in Law Number 31 of 2014 regarding

---

[6] Steve Van De Weijer, Rutger Leukfeldt, And Sophie Van Der Zee, "Reporting Cybercrime Victimization: Determinants, Motives, And Previous Experiences," *Policing* 43, No. 1 (2020): 17–34, Https://Doi.Org/10.1108/Pijpsm-07-2019-0122.

[7] Jildau Borwell, Jurjen Jansen, And Wouter Stol, "The Psychological And Financial Impact Of Cybercrime Victimization: A Novel Application Of The Shattered Assumptions Theory," *Social Science Computer Review* 40, No. 4 (2022): 933–54, Https://Doi.Org/10.1177/0894439320983828.

[8] Maria Grazia Porcedda And David S. Wall, "Modelling The Cybercrime Cascade Effect In Data Crime," In *Proceedings - 2021 Ieee European Symposium On Security And Privacy Workshops, Euro S And Pw 2021*, 2021, 161–77, Https://Doi.Org/10.1109/Eurospw54576.2021.00025.

[9] Rahayu Ahmad And Ramayah Thurasamy, "A Systematic Literature Review Of Routine Activity Theory's Applicability In Cybercrimes," *Journal Of Cyber Security And Mobility*, 2022, Https://Doi.Org/10.13052/Jcsm2245-1439.1133.

[10] Yudha Chandra Arwana, "Victims Of Cyber Crimes In Indonesia: A Criminology And Victimology Perspective," *Semarang State University Undergraduate Law And Society Review* 2, No. 2 (2022): 181–200, Https://Doi.Org/10.15294/Lsr.V2i2.53754.

Amendments to Law Number 13 of 2006 concerning Witness and Victim Protection, every victim of crime has the right to protection.[11]

The risk of system failure and/or the possibility of electronic crime (cybercrime) committed by irresponsible individuals seeking profit will always cast a shadow over the banking industry's use of information technology to innovate banking service products. Natural disasters can also contribute to system failure on a larger scale. Examples of system malfunctions include server outages. In the meantime, there has been a noticeable rise in cybercrime in Indonesia's banking sector. This includes identity theft, carding, hacking, cracking, phishing, viruses, cybersquating, ATM fraud, and other crimes.

Customers who bank with banks and the banking industry are negatively impacted by the high crime rate of phishing fraud in financial institutions. Customers require a high level of system security the higher the crime rate is, as many attackers and phishers are interested in taking advantage of customer data if the security is inadequate. Phishers can perform their actions with various media, namely email, SMS, WhatsApp text, and Telegram which can lead their victims to actions that lead to losses.

A previous study on the legal protection for victims of cybercrime as a form of transnational crime has extensively examined the global impact of globalization on cybercrime. Jones et al. (2018) highlighted the importance of cross-border cooperation and the development of a coherent legal framework to protect victims. They pointed out that the lack of harmonization in international legal regulations could be a serious obstacle in effectively combating cybercrime.[12]

Regarding the legal defense of victims of transnational cybercrime, a previous study by O Sviatun provided an in-depth perspective on the legal challenges faced by countries in addressing cybercrime. They emphasized the need to develop legal mechanisms capable of adapting to the evolving dynamics of cybercrime.[13]

Further research by Theodore Longtchi et al discussed the impact of cybercrime on victims at both an individual and societal level. They stressed that legal protection should not only involve prevention and enforcement efforts but also rehabilitation and support for victims to recover from the psychological and economic consequences of cybercrime.[14]

In addition, in this case the development of electronic transactions is increasing and cannot be separated from the presence of various problems, especially in protecting consumers from personal data being misused by a number of individuals in Indonesia, where financial providers do not register and the government, in this case the OJK, has not given permission. This ultimately causes supervision and protection of consumers to

---

[11] Situngkir, "Asas Legalitas Dalam Hukum Pidana Nasional Dan Hukum Pidana Internasional."
[12] C. Jones, A., Smith, B., & Johnson, "Globalization And Cybercrime: The Need For International Legal Cooperation 10," *International Journal Of Cybersecurity*, (2), (2018): 145–62.
[13] O Sviatun Et Al., "Combating Cybercrime: Economic And Legal Aspects," *Wseas Transactions On Business And Economics* 18 (2021): 751–62.
[14] Theodore Longtchi Et Al., "Internet-Based Social Engineering Attacks, Defenses And Psychology: A Survey," *Arxiv Preprint Arxiv:2203.08302*, 2022.

weaken. Thus, it will cause crucial problems, including violations of personal data, one of which is hacking access to consumers' telephone contacts.

Based on the phenomenon of the above cases related to the rise of transnational crimes, especially in cybercrime cases, it is necessary to establish strict legal protection for victims of electronic information and transaction crimes. Therefore, this article aims to provide solutions and education for the public to be more cautious in engaging in online transactions. Additionally, the research seeks to encourage the government to implement legal measures that ensure the protection of victims and instill a deterrent effect on criminals.

2. METHOD

This study employs both a conceptual and statutory approach to normative juridical research. A literature approach is being used in normative juridical research, which involves an analysis of relevant journals, books, laws, and other documents. Normative legal science is closely associated with legal practice, which is focused on two primary facets: the creation and implementation of laws.[15]

The three (three) legal materials that comprise this study are primary, secondary, and tertiary. Primary legal materials include provisions pertaining to legal protection for victims of cybercrime, a subset of transnational crime. Encyclopedias and the internet are examples of tertiary legal materials, whereas books, journals, articles, and other non-official legal publications are considered secondary legal materials. The application of a literature study model to the process of obtaining legal documents.[16]

Content analysis is the method used for legal material analysis (content analysis technique). Any methodical process that aims to investigate the information's content is called content analysis. This analysis is centered on all of the acquired secondary data. Following the acquisition of the relevant data, this paper conducts a logical, methodical, and legal analysis of the data. When data is analyzed logically, it follows the rules of deductive logic, which entails extrapolating conclusions from a general problem to the specific issues at hand. Systematic data analysis refers to the process of connecting and relating dependent and interconnected data sets. Additionally, the data is analyzed legally,

---

[15] Rusli Hadijan, "'Metode Penelitian Hukum Normatif: Bagaimana?,'" *Law Review, Fakultas Hukum Universitas Pelita Harapan* 5, No. 3 (2006): 50.

[16] Kornelius Benuf And Muhamad Azhar, "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer," *Gema Keadilan* 7, No. 1 (2020): 20–33, Https://Doi.Org/10.14710/Gk.7.1.20-33.

meaning that it begins with the regulations that are currently in place and is linked to the positive laws that are currently in effect.

3. RESULTS AND DISCUSSION

Legislation Protecting Victims of Phishing as a Transnational Crime

Cybercrime can disrupt and threaten a country's national security because many countries have connected their data and control over several sectors through the internet or online. Due to the wide range of cybercrimes that can occur on the internet, there is no definitive classification and definition of cybercrime. However, cybercrime has gained international attention as one of the transnational crimes.

Benjamin dan michal[17] highlight the significance of multilateralism in addressing global issues, including those related to the realm of global public health and environmental and energy issues. However, Mugarura & Ssali[18] point out that the current global strategies to deal with cybercrimes are fragmented, lacking a coherent global approach. This fragmented nature of global strategies is further emphasized by Onomrerhinor[19], who talks about how cybercrimes are transnational in nature and how international cooperation is necessary to remove safe havens for these types of crimes. Given these difficulties, Rowe[20] suggests that a multilateral international treaty be created expressly to deal with state-sponsored cybereconomic espionage that is conducted across borders. This suggests that a comprehensive and coordinated legal framework at the international level is essential to effectively combat cybercrimes. Such a treaty could provide a unified approach to addressing cybercrimes that are sponsored by states and operate across national boundaries.

Julian Droogan stated that cybercrime has evolved into one of the main threats to the well-being of people around the world.[21] As such, it proves that security aimed at preventing and dealing with cybercrime needs to be developed and become the nation's new area of national security emphasis.

The laws that protect victims of phishing as a transnational crime are explained in the following manner: First, the Law Number 19 of 2016 Concerning Amendments to Law Number 11 of 2008 Concerning Electronic Information and Transactions; the creation of the ITE Law is one way that Indonesian criminal law is implemented to enforce jurisdiction against cybercrimes. The ITE Law was created expressly to control a range of

---

[17] Benjamin Faude And Michal Parizek, "Contested Multilateralism As Credible Signaling: How Strategic Inconsistency Can Induce Cooperation Among States," *Review Of International Organizations* 16, No. 4 (2021): 843–70, Https://Doi.Org/10.1007/S11558-020-09398-7.

[18] Norman Mugarura And Emma Ssali, "Intricacies Of Anti-Money Laundering And Cyber-Crimes Regulation In A Fluid Global System," *Journal Of Money Laundering Control* 24, No. 1 (2020): 10–28, Https://Doi.Org/10.1108/Jmlc-11-2019-0092.

[19] Flora Alohan Onomrerhinor, "Eliminating Safe Havens For Transnational Cybercrimes In The African Continental Free Trade Area," *Journal Of Intellectual Property And Information Technology Law (Jipit)* 2, No. 1 (2022): 49–81, Https://Doi.Org/10.52907/Jipit.V2i1.206.

[20] Brenda I. Rowe, "Transnational State-Sponsored Cyber Economic Espionage: A Legal Quagmire," *Security Journal* 33, No. 1 (2020): 63–82, Https://Doi.Org/10.1057/S41284-019-00197-3.

[21] Arnold Sotarduga Silangit, Laili Furqoni, And Fanny Tanuwijaya, "Perlindungan Hukum Terhadap Korban Penganiayaan Yang Dilakukan Oleh Oknum Polri Saat Aksi Demonstrasi," *Interdisciplinary Journal On Law, Social Sciences And Humanities*, 2022, Https://Doi.Org/10.19184/Idj.V3i1.29497.

human activities in the area of information and communication technology, including a number of offenses classified as cybercrimes. Nevertheless, in addition to the ITE Law, other laws and regulations also expressly or implicitly regulate cybercrime, depending on the extent and classification of cybercrime. The legalization of cybercrime in Indonesia has consequences for the country's and the global community's efforts to combat cybercrime.

One of the banking services that is a type of information technology development is the Internet banking system, and Law No. 19/2016 on the Amendment to Law No. 11/2008 on Information and Electronic Transactions is thought to be able to regulate the legal issues surrounding it. Although there are articles in the ITE Law that regulate transactions with Internet media, rather than Internet banking specifically, obstacles like technological and legal aspects are no longer a factor impeding the development of Internet banking in Indonesia.

Every provider of an electronic system is accountable for ensuring that the system functions as intended and is obligated to offer a dependable and secure system. When an electronic system is considered reliable, it means that its capabilities meet the needs of its users. A secure electronic system is one that is both physically and virtually guarded. When an electronic system is functioning correctly, it can perform as specified by its specifications. Furthermore, the introduction of the electronic system.[22] Responsible refers to the existence of a legal subject with implementation rights for the electronic system. This clause, however, does not apply if it can be demonstrated that an electronic system user's negligence, fault, or force majeure occurred.[23]

Unless otherwise specified by another law, every operator of an electronic system is required by the ITE Law to operate a system that satisfies a set of minimum requirements. First and foremost, the system must have the ability to retrieve electronic data and/or documents in their entirety while closely following the retention period required by applicable laws and regulations. Furthermore, it is imperative to ensure the protection of electronic information's availability, integrity, authenticity, confidentiality, and accessibility throughout the system's operation. Thirdly, it is crucial to strictly follow established protocols or guidelines that control how the electronic system operates. Furthermore, the system needs to use language, data, or symbols that all parties involved in the implementation of electronic systems can easily understand in order to provide instructions or processes. Lastly, to ensure the procedure or product's continued relevance and efficacy, a continuous mechanism is needed to preserve its novelty, clarity, and accountability. When taken as a whole, these ideas support the dependability and resilience of electronic systems.

---

[22] Muhammad Farid, "Penyebarluasan Informasi Mengenai Bentuk Dan Macam Tindakan Cyberbullying Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dan Upaya Pencegahannya Melalui Keb," *Jurnal Sumbangsih*, 2020, Https://Doi.Org/10.23960/Jsh.V1i1.11.

[23] Ahmad Junaedy Tarigan, Adil Akhyar, And Mustamam Mustamam, "Perlindungan Hukum Terhadap Korban Pornografi Dalam Media Sosial Perspektif Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik," *Jurnal Ilmiah Metadata*, 2023, Https://Doi.Org/10.47652/Metadata.V5i1.318.

The second is Law No. 27 of 2022 on Personal Data Protection. This law was finally passed by Indonesia in 2019 after much anticipation, giving peer-to-peer lending fintech users more legal protection and clarity. Given the increase in data breaches, the law's timing is ideal because it aims to safeguard citizens' rights to privacy, increase public awareness of the importance of data protection, and guarantee that these rights are upheld.

This legislation is anticipated to provide a robust legal foundation for the management and safeguarding of individuals' and public servants' personal information. Information privacy is one of the human rights associated with personal safety. This right to personal protection is guaranteed by Article 28G of the 1945 Constitution. This privacy or personal security is universal in the sense that many nations recognize it.

In accordance with Article 26, unless specified otherwise by Laws and Regulations, the utilization of any information via electronic media concerning an individual's personal data should only occur with the explicit consent of the respective individual. The legal safeguard provided for personal data protection under the ITE Law is linked to the personal rights (privacy) of the affected party. To ensure legal certainty for individuals who believe their privacy has been violated, it is imperative to endorse Law Number 27 of 2022 concerning Personal Data Protection. The Ministry of Communication and Information has published an academic paper on Law No. 27 of 2022 related to Personal Data Protection on the BPHN website. This action is in accordance with Article 5 of Law No. 12/2011 on the Formation of Legislation, emphasizing the need for implementation in compliance with the stipulations of sound laws and regulations.

As a result, the analysis that was conducted in this case was predicated on an examination of the fundamentals of creating effective laws and regulations in order to gain public acceptance of Law Number 27 of 2022 concerning the protection of personal data: Making sure that the purpose of the law is clear is essential to creating legislation that works. The creation of personal data protection laws, which are specifically intended to protect Indonesian citizens' right to privacy and their personal information, serves as an excellent example of this concept. The DPR or other government agencies with legislative authority must pass the Personal Data Protection Law as soon as possible in order to enact such laws, which calls for the intervention of a legislative body. Every piece of legislation must, beyond the legislative process, exert control over social norms at the philosophical, sociological, and legal levels. The proposed Personal Data Protection Law has the potential to bring about positive social changes by giving people the ability to take legal action if their personal information is disclosed. This could entail bringing legal action, pressuring online retailers to give justification, or getting the government involved to find and fix data leaks. Moreover, the necessity and usefulness of laws and regulations in governing society, the state, and the country determines their efficacy and efficiency. The Personal Data Protection Law, which addresses new flaws in internet security systems and offers a vital framework to traverse the unpredictable terrain of data leaks, is essential given the increasing complexity of technology and the internet.

Based on the analysis above, it is possible to view the implementation of the Personal Data Protection Law as a solution to stop data leakage. Legal clarity will also benefit

Indonesians. Law No. 8/1999 lists nine consumer rights, but given the importance of consumer protection, the fifth right—"The right to adequate defense, protection, and settlement of consumer protection disputes"—is the most crucial. data leaking. The protection that customers may have extends to the protection of personal data kept on e-commerce websites, even though it isn't stated clearly.

Article 51 of Law No. 27 of 2022, which particularly targets individuals accountable for identity theft, outlines the prohibited matters pertaining to Personal Data Protection. Article 51 of the Personal Data Protection Law is broken by those who divulge personal information for personal gain. Moreover, criminal penalties may be applied in accordance with Article 61 of Law No. 27 of 2022 relating to Personal Data Protection for violations of Article 51 of Law No. 27 of 2022 relating to Personal Data Protection.[24]

Legal Protection for Victims of Cyber Crime as a Form of Transnational Crime

Cybercrime is the term used to describe illegal activity involving computers or computer networks that are used as instruments, targets, or locations for criminal activity. In essence, law is a set of rules governing people's attitudes toward actions and behaviors, which the state penalizes those who break. Despite the fact that the cyber world is virtual, laws are still required to control community behavior, if for no other reason than two: First of all, the online community is just like the real community; it has shared values and interests that need to be safeguarded on an individual and collective level. Second, despite taking place online, community transactions have an impact in the real world on both an economic and non-economic level.[25]

At the moment, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions serves as the regulation that serves as the foundation for legal proceedings involving cybercrime. It is hoped that the ITE Law will protect Indonesians who use information technology; this is crucial given the country's growing annual population of internet users. The growing use of the internet has both positive and negative effects on people's lives. While it can be very convenient for some people to carry out their daily tasks, it also makes it easier for some people to commit crimes. In fact, a lot of crimes these days use information technology. Due to the fact that cybercrime differs somewhat from other crimes in general, it is a rapidly expanding phenomenon that needs to be closely monitored. There are several ways that third parties committing ITE crimes could cause victim loss in banking transactions. Nonetheless, the bank should take certain steps to safeguard the interests of its clients, such as using government and self regulators.

Initially, there is self-regulatory legal protection; in the implementation of online banking services, there is preventive legal protection of victims' personal data through

---

[24] Csa Teddy Lesmana, Eva Elis, And Siti Hamimah, "Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia," *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia*, 2022, Https://Doi.Org/10.52005/Rechten.V3i2.78.

[25] Meslik Anin, "Perlindungan Hukum Terhadap Nasabah Bank Korban Cyber Crime Dalam Internet Banking Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *Iustitia Omnibus (Jurnal Ilmu Hukum)*, 2020.

internal legal regulatory action from the online banking service provider itself. through the need for registration. It is accessible via the online banking service if this step has been completed. Internet banking services, then, serve as a vehicle for product promotion while also serving as a means of enabling online transactions. Hackers can't access the victim's personal information if this preventive measure is taken. The time out session method is used to increase security; if there is no victim activity for ten minutes, access will become inactive.

Second, legal protection through government regulation: Law Number 10 of 1998 has various provisions pertaining to banking, including paragraphs 1 and 2 of article 40 and paragraph 29. In paragraph 5 of article 29, it states that "for the benefit of customers the bank provides information regarding the possibility of the risk of loss for the victim's transaction conducted through the bank" . According to this article's explanation, the bank operates with public funds that are deposited there because of trust. As a result, each bank needs to preserve both its health and the public's confidence. The Electronic Transaction Law contains certain provisions that can serve as a foundation for the legal protection of victims' personal data when internet banking is implemented. Legal protection in the business world, particularly in banking, is always centered on how the financial sector's organizers safeguard clients or consumers. One of the pillars of the development of consumer protection is the consumer's position vis-à-vis business actors: Assuming a balanced relationship between business actors and consumers, the tenet of "let the buyer beware" or caveat emptor serves as the foundational principle. This theory, however, ignores the changing environment in which consumers frequently lack sufficient information to make wise decisions. Consumer losses may arise from inadequate product knowledge or a lack of transparency on the part of business actors, who may attempt to shift the blame by blaming the customer for their own carelessness.

In contrast, the theory of due care asserts that business entities have an obligation to exercise caution when promoting their goods or services. This doctrine absolves the business actor of responsibility so long as they take reasonable steps to ensure the quality of the product. In accordance with the evidentiary principle of Indonesian private law, which requires the plaintiff to provide evidence to support their claims, the burden of proof rests with the party presenting the case. According to the privity of contract doctrine, corporate actors have a duty to safeguard customers, but only after a contractual relationship has been established. Companies are only liable for the things they expressly guarantee, and customers have the right to take legal action if a contract is broken. This principle is consistent with BW Article 1340, which states that an agreement's validity is limited to the parties that participated in its formation. Customers can therefore pursue legal action within the bounds of the existing contractual arrangement..[26]

As a matter of state law, the state of Indonesia owes all Indonesians a duty of community protection. The Preamble of the 1945 Constitution's fourth paragraph, which states that the state has the ideals to protect the Indonesian people so that every community

[26] S Ismantara And Y Prianto, "Relevansi Hukum Perlindungan Konsumen Indonesia Di Era Ekonomi Digital," *Prosiding Serina*, 2022.

that requires legal protection can realize their rights as citizens of Indonesia, particularly those who are victims of crime, also captures the essence of protection from the state.

According to Article 28 D(1) of the 1945 Constitution, every individual is entitled to the right of recognition, guarantees, protection, and certainty under a just law, ensuring equal treatment before the law. This provision has been legally mentioned for the protection of losses suffered by victims. This constitutional clause is the cornerstone that protects each and every individual's legal rights within the jurisdiction.

Article 3, paragraph (2) of Law No. 39/1999 on Human Rights highlights that each and every person has the right to legal recognition, protection, guarantees, fair treatment, legal certainty, and equal treatment before the law. This serves to further reinforce these principles. The dedication to protecting human rights and guaranteeing justice and equality in legal matters is highlighted by this statutory inclusion.

Furthermore, as stated in Article 40, paragraph (2) of the Information and Electronic Transactions (ITE) Law, the government is required to safeguard the public interest against disruptions resulting from the improper use of electronic information and transactions. Maintaining public order is included in this protection, and it must be done so in compliance with all applicable laws and regulations. Fairness, protection, and equality before the law are fundamental legal principles that are upheld by the ITE Law, which is an example of the legal framework designed to address issues brought about by the improper use of electronic information and transactions.

Article 1 Point 8 of Law Number 31 of 2014 Concerning the Amendment to Law Number 13 of 2006 Concerning Witness and Victim Protection reads as follows: "In order to give Witnesses and/or Victims a sense of security, protection refers to all efforts made by LPSK or other institutions in compliance with the provisions of this Law to fulfill their rights and provide assistance."

Barda Nawawi Arief mentions the protection of victims, stating that the term has two meanings, specifically: First of all, it might be seen as a preventative step to protect people from falling prey to crimes. According to this interpretation, legal frameworks play a proactive role in preventing potential wrongdoers and fostering an atmosphere of safety for people. Laws act as a deterrent, preventing criminal activity and protecting people from harm by precisely defining and enforcing boundaries.

Second, after an incident, victims may utilize legal protection as a means of obtaining support and compensation. In this situation, the focus switches to making sure victims get assurances and fair compensation for the losses they suffer. This could involve a range of reparations, including programs for rehabilitation and actions to bring about mental equilibrium, which might entail forgiving someone. In addition, legal protection includes monetary compensation, which recognizes the harm caused by the crime and aims to lessen the victims' burdens. This dual interpretation emphasizes how comprehensive legal protection is, covering both deterrent strategies and avenues of assistance for individuals impacted by criminal activity.[27]

---

[27] Damasha Khoiri Clevalda, "Perlindungan Hukum Terhadap Nasabah Bank," *Privat Law*, 2021.

Since the Indonesian state was established as a state of law, law enforcement serves to demonstrate the ultimate purpose of the law, which is to establish order and peace in society through the application of the law and legal protections. Law enforcement is a situation that balances legal rules from noble values to actions born in the midst of social life. Analyzing cybercrime activity pertaining to hacking and eavesdropping on the WhatsApp app is a cybercrime case. Khasanah & Sutabri[28] talk about how cybercrimes involving illegal access and communication interception on the WhatsApp platform are analyzed. This case serves as an example of the illegal activity that takes place in the cyberspace, underscoring the necessity of strong legal measures to deal with these kinds of offenses.

Furthermore, the study of cybercrime in the context of Sharia banking systems, as discussed in the literature review by Aghniya[29], offers one more specific illustration. This analysis highlights the transgressive nature of cybercrimes and the need for legal frameworks designed to address these particular challenges by shedding light on the specific vulnerabilities and criminal activities within the financial sector. These instances highlight the variety of cybercrimes and the urgent requirement for all-encompassing legal measures to successfully prosecute such offenses. The cases also demonstrate how crucial it is to comprehend the particular environments in which cybercrimes take place and the consequences for legal and regulatory responses in order to guarantee the safety of people and organizations from cyberthreats.

Cyber crime or in other terms, cybercrime in the regulations for electronic transactions, namely the ITE Law, does not clearly regulate the form of protection for victims of crime in an electronic transaction. Cyber crime in banking is a type of crime that can cause material losses to its victims, such as personal data. Basically, personal data is protected under Indonesian laws and regulations. Therefore, when the confidentiality of a property right is no longer perfect, it requires legal protection in the form of protection to the parties who are harmed. Because when personal data is known by other parties, it can result in a breach of the data, such as what is rampant, namely the perpetrator's interest in credit card data and / or account numbers so that it can create economic losses for the victim.

However, according to the ITE Law, the form of fulfillment of the right to protection for victims in an electronic transaction or cyber crime is only marked by the form of case settlement in the form of criminal provisions for acts prohibited in this law to the perpetrators of criminal acts which are listed from Article 45 to Article 52 of the ITE Law in the form of imprisonment and/or fines. Punishment of the perpetrator to enforce the law for the victims is the right step so that most forms of criminal provisions listed in the ITE Law and the Criminal Code are coupled with sanctions in the form of imprisonment and

---

[28] Nurul Khasanah And Tata Sutabri, "Analisis Kejahatan Cybercrime Pada Peretasan Dan Penyadapan Aplikasi Whatsapp," *Blantika : Multidisciplinary Journal* 2, No. 1 (2023): 44–55, Https://Doi.Org/10.57096/Blantika.V2i1.13.

[29] "Studi Literatur Kejahatan Siber Pada Sistem Perbankan Syariah Di Era 4.0," *Aghniya: Jurnal Ekonomi Islam* 4, No. 2 (2022), Https://Doi.Org/10.30596/Aghniya.V4i2.12759.

fines. So that in the end, imprisonment and fines for the perpetrators of criminal acts are deemed insufficient to protect and fulfill the rights of victims, especially for victims of cyber crime to compensate material losses that they should not experience, especially for victims who have a weak economy.

Regarding regulations that specifically regulate the protection of victims, in Indonesia there are laws and regulations that regulate it, namely in Law No. 31 of 2014 concerning Amendments to Law No. 13 of 2006 concerning Witness and Victim Protection accompanied by LPSK or the Witness and Victim Protection Agency which is an active institution to assist witnesses and / or victims of criminal acts to obtain protection and fulfillment of their rights. Victims of ITE crimes basically have a need to fulfill the material losses they experience, in the Law on Witness and Victim Protection or called the UUPSK states that there is protection for victims and / or witnesses of criminal acts, namely in the form of Compensation, Restitution and Assistance. For material losses for victims of cyber crime, Restitution is the right method. As in Article 1 Point 11 which states that "Restitution is compensation given to the victim or their family by the perpetrator or third party."

The potential for ITE crime victimization is a type of operational risk. Operational Risk according to Article 1 Item 7 of the Financial Services Authority Regulation Number 18/POJK.03/2016 concerning the Implementation of Risk Management for Commercial Banks is the risk due to inadequate and/or malfunctioning internal processes, human error, system failure, and/or external events that affect bank operations. Michel Crouhy, Dan Gali and Robert Mark define operational risk as a risk related to business operations which includes 2 (two) risk components. The first is operational failure or internal risk which consists of risks originating from human resources, processes and technology. The second is operational strategy risk or external risk that comes from factors such as politics, taxes, regulations, society and competition.[30]

In addition, victims of the aforementioned unfavorable events who have suffered harm must be protected, necessitating efforts to find solutions. Repressive protection is defined as protection whose goal is to settle arising issues or disputes.[31] There are essentially two models of approaches that can be used to protect cybercrime victims legally: 1) the procedural rights model, in which the victim has the right to participate in all stages of the legal process and can help the prosecutor in carrying out prosecutions; 2) the service model, which views the victim as a person who needs to be served by the police and other law enforcement officials in order for the victim to feel that his interests are protected in a fair manner. Aiding victims of cybercrime and physical crimes needs to happen at every stage of the investigation, trial, and post-trial phases of the process.

---

[30] Karen A. Horcher, *Essentials Of Financial Risk Management*, *Essentials Of Financial Risk Management*, 2005, Https://Doi.Org/10.1002/9781118386392.

[31] Indra Utama, "Perlindungan Hukum Terhadap Debitur (Nasabah) Dalam Perjanjian Kredit Tanpa Agunan Ditinjau Dari Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen," *Islamic Circle*, 2021, Https://Doi.Org/10.56874/Islamiccircle.V1i2.288.

Regarding Indonesia's legal protection for victims of information crimes and electronic transactions, the author compares Singapore, Malaysia, and the United States' law enforcement practices for protecting victims of information crimes and electronic transactions with regard to the protection of personal data.

Based on the Global Cybersecurity Index (GCI) survey in 2017, Singapore is considered the best country in terms of cybersecurity implementation. Singapore's journey in cybersecurity began a decade ago with the adoption of a cybersecurity masterplan in 2005. This initial master plan was implemented over three years through a multi-stakeholder approach and focused on protecting individual, public and private data. In addition to building infrastructure, the master plan also emphasizes human resource development through capacity building programs to increase understanding and awareness of cybersecurity issues.[32]

In the context of Indonesia, the GCI plays a significant role in assessing the country's cybersecurity maturity and its impact on various aspects of governance, economic growth, and political stability. Indonesia's ranking in the GCI is particularly noteworthy, with the country being ranked 24th in the Global Cybersecurity Index (GCI). This ranking provides valuable insights into Indonesia's cybersecurity posture and its standing in the global cybersecurity landscape. Furthermore, the GCI is instrumental in understanding the impact of cybersecurity on political stability, as evidenced by its correlation with the level of political stability based on the Political tability and Absence of Violence/Terrorism indicator of the Worldwide Governance Index.[33] This highlights the interconnectedness of cybersecurity with broader governance and political phenomena. The GCI also serves as a critical measure for assessing the impact of national competitiveness on economic growth and income levels, as demonstrated by its use as a proxy for national competitiveness and productivity in empirical analyses.[34] Additionally, the GCI's influence on human development and the forming factors, particularly in the context of AEAN countries, underscores its significance in shaping regional cybersecurity and development agendas.[35]

Singapore unveiled its cybersecurity strategy later in 2016, with four main objectives in mind: bolstering critical infrastructure, assuming shared accountability for cybersecurity, creating a thriving ecosystem for cybersecurity, and enhancing global cybersecurity cooperation. The Personal Data Protection Act (PDPA), which was passed by Singapore in 2012, provides the legal framework for the protection of personal data

---

[32] Infocomm Media Development Authority (Imda), "Singapore Gears Up For Cyber Security [Daring] Imda.," imda, 2017, Https://www.imda.gov.sg/About/Newsroom/Archived/Ida/Media Releases/2005/20050712110643.

[33] Tuan Anh Nguyen Et Al., "Effects Of 'Digital' Country's Information Security On Political Stability," *Journal Of Cyber Security And Mobility* 11, No. 1 (2022): 29–52, Https://Doi.Org/10.13052/Jcsm2245-1439.1112.

[34] Aziz Sodikov Et Al., "Impact Of National Competitiveness On Economic Growth And Income Level – Evidence From The Selected Post-Soviet Countries," *Research In World Economy* 12, No. 2 (2021): 17, Https://Doi.Org/10.5430/Rwe.V12n2p17.

[35] Edy Suandi Hamid, "Human Development Index And The Forming Factors: The Effect Of Global Competitiveness Index In Ten Asean Countries," *Journal Of International Business And Economics* 7, No. 2 (2019), Https://Doi.Org/10.15640/Jibe.V7n2a7.

there. The principles of protecting personal information, gathering, using, and disclosing it, as well as maintaining it and allowing access and correction, are all fully regulated by law. In addition, the law requires the creation of the Personal Data Protection Commission (PDPC), which will serve as the oversight and enforcement authority for the PDPA. One of the complaints leveled against the PDPA is that, since it does not apply to the government, it is difficult to define the government's jurisdiction and set limits on how personal information from internet users is used in Singapore.[36]

In addition, the PDPA does not contain any classification of personal data as in the EU GDPR and South Korea PIP Law as explained above. Nonetheless, the PDPA has an important and clear role in terms of personal data protection that should be emulated by other countries around the world. The strictness of personal data protection regulations in Singapore does not mean that misuse of user data has disappeared completely. Interestingly, PDPC recapitulates all allegations and breaches of the PDPA on its website so that the data is easily accessible to the public. This shows that the PDPC as the authorized party takes all personal data protection violations seriously regardless of the size of the threat posed. For example, the PDPC gave the National University of Singapore (NUS) an ultimatum of 120 days to train its students in personal data protection.[37]

This action was taken after the PDPC discovered that hundreds of NUS freshmen's personal data (full names, cell phone numbers, food preferences, email addresses, etc.) that were originally stored in the cloud computing service Google Sheets spreadsheet eventually spread to the public due to the carelessness of one of the unidentified document owners to change the rules of the document to make it freely accessible to the public. In addition, PDPC also did not hesitate to give a fine of S$10,000 to large companies such as JP Pepperdine Group and Propnex Reality who neglected to maintain the privacy of their user data on their respective sites so that it could be seen by the public. However, Singapore is also not spared from the Cambridge Analytica scandal. This case is currently the concern of the PDPC and in-depth investigations are still being carried out.

The United States is ranked second in the world for cybersecurity, behind only Singapore, according to the 2017 GCI survey. The United States plays a crucial role in internet governance as a regulator and an actor. In order to achieve fairer and more transparent internet governance, the internet was first regulated by the US Ministry of Defense before being eventually turned over to international non-state organizations like ICANN, ITU, and so forth through political lobbying and collaboration between stakeholders worldwide. It is peculiar that the United States, the nation that gave rise to the internet, lacks a federal law that expressly addresses the safeguarding of personal information. The Comprehensive National Cybersecurity Initiative was launched by the US government in 2008 under President George W. Bush. It is merely intended to act as a set

---

[36] Ministry Of Communications And Information, "Singapore's Cybersecurity Strategy 2016 [Daring] Ministry Of Communications And Information.," 2016, Https://www.csa.gov.sg/News/Publications/Singapore-Cybersecurity-Strategy, .

[37] Personal Data Protection Commssion (Pdpc) Singapore., "Who We Are [Daring] Pdpc Singapore," accessed November 10, 2023, Https://www.pdpc.gov.sg/About-Us/Who-We-Are, .

of guidelines for the creation of a cybersecurity framework within the US. The remaining personal data protection laws in the US were created by individual states and particular public/government industries (like the banking and health sectors). It is feared that this disjointed legal system will result in conflicting laws and fall short of its obligation to safeguard internet users' data security.[38]

Also, the United States does not have a specialized agency that handles personal data protection. Issues related to data security are mostly held by the Federal Trade Commission (FTC). Despite this, the United States scored 1 for legal aspects and 0.96 for technical aspects in the 2017 GCI assessment. The reason behind the United States' high score in legal aspects is attributed to some central government actions that are able to link sectoral policies. For example, the establishment of the Resource Center for State Cybersecurity as a forum for stakeholders at the state level to coordinate, provide information and advocate to other states in dealing with cybersecurity issues. In addition, the United States also has the US Cybersecurity Information Sharing Act (CISA) 2015. An interesting element of this regulation is the flexibility for government, private and individual parties to cooperate in sharing information about cybersecurity threats.[39]

Malaysia is a country that ranked third in the GCI in 2017 after Singapore and the United States. Cybersecurity development efforts have started as early as 1997 through the establishment of the Malaysian Computer Emergency Response Team (MyCERT) or now known as Cybersecurity Malaysia. It is a government organization under the Ministry of Science, Technology and Innovation responsible for cybersecurity in Malaysia as well as promoting internet safety among internet users in Malaysia.[40]

In the context of personal data protection, in 2000, the Malaysian government introduced a Personal Data Protection Bill which was drafted based on the European Data Protection Standards, although the Bill was ultimately not tabled in Parliament due to strong opposition from the communications and multimedia industries. The discussion on the Personal Data Protection Bill in Malaysia has come a long way, until finally in 2010, the Personal Data Protection Act (PDP Act 2010) was enacted. The PDP Act 2010, which consists of 146 articles, is arguably quite specific in regulating the protection of personal data. Some of the important points regulated in the law relate to the classification of personal data, the principles of personal data protection, the rights of data owners, the establishment of specialized agencies related to personal data protection, and law enforcement procedures related to violations and crimes related to personal data. The 2010 PDP Law focuses on the processing of personal data in commercial transactions and to prevent the misuse of personal data.

Despite having a dedicated institution to carry out the Act and a legal foundation for protecting personal data, Malaysia appears to be experiencing issues with its execution.

---

[38] N O'connor, "Reforming The Us Approach To Data Protection And Privacy [Daring].," Council On Foreign Relations., 2018, Https://www.cfr.org/Report/Reforming-Us-Approach-Data-Protection, .

[39] Dla Piper, "Data Protection Laws Of The World: United States [Daring].," Dla Piper, accessed November 10, 2023, Https://www.dlapiperdataprotection.com/Index.Html?T=Law&C=Us, .

[40] Cybersecurity Malaysia, *Laporan Tahunan Cybersecurity Malaysia* (Selangor: Darul Ehsan, 2011). Hlm. 30-31.

This is due in part to the fact that the PDP Act of 2010's definition of personal data is based on information pertaining to business transactions, meaning it cannot cover personal data unrelated to business transactions, and business transactions are defined broadly. As a matter of fact, the broad definition of commercial transactions—which encompasses the collection, recording, storage, and even all actions related to personal data—creates uncertainty for data holders (data users), according to research by Malaysian legal academic Noriswadi Ismail. (such as organizing data, adapting, opening data, and sending and exchanging data). Furthermore, there's the matter of Cambridge Analytica's intervention in the Malaysian elections, which undoubtedly demonstrates the improper use of Malaysian citizens' personal data.[41]

4. CONCLUSION

From the above analysis the author draws the following conclusions: 1) Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions and Law Number 27 of 2022 concerning Personal Data Protection previously regulated regulations legislation that protects victims of information crimes and electronic transactions as transnational crimes. 2) As a type of transnational crime, legal protection for victims of cyber crime basically has two types of approaches that can be applied, namely: 1) procedural rights model where victims are allowed to participate more actively in the prosecution process and have the right to be present at all stages legal system; and 2) a service model where victims are considered as people who need to be looked after by the police and other law enforcement officials so that their rights can be upheld in a just environment. Providing assistance to victims of cybercrime and physical crime needs to be carried out at every stage of the investigation, trial and post-trial process.

BIBLIOGRAPHY

Ahmad, Rahayu, and Ramayah Thurasamy. “A Systematic Literature Review of Routine Activity Theory’s Applicability in Cybercrimes.” *Journal of Cyber Security and Mobility*, 2022. https://doi.org/10.13052/jcsm2245-1439.1133.

Angkasa, Angkasa, and Rili Windiasih. “Cybercrime Di Era Industri 4.0 Dan Masyarakat 5.0 Dalam Perspektif Viktimologi.” *Journal Justiciabelen (Jj)* 2, no. 2 (2022): 104. https://doi.org/10.35194/jj.v2i2.2113.

Anin, Meslik. “Perlindungan Hukum Terhadap Nasabah Bank Korban Cyber Crime Dalam Internet Banking Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.” *Iustitia Omnibus (Jurnal Ilmu Hukum)*, 2020.

Arwana, Yudha Chandra. “Victims of Cyber Crimes in Indonesia: A Criminology and Victimology Perspective.” *Semarang State University Undergraduate Law and Society Review* 2, no. 2 (2022): 181–200. https://doi.org/10.15294/lsr.v2i2.53754.

Benuf, Kornelius, and Muhamad Azhar. “Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer.” *Gema Keadilan* 7, no. 1 (2020): 20–33. https://doi.org/10.14710/gk.7.1.20-33.

[41] Mohamad Intan Sabrina And Irma Ruslina Defi, “Telemedicine Guidelines In South East Asia—A Scoping Review,” *Frontiers In Neurology* 11 (2021): 581649.

Borwell, Jildau, Jurjen Jansen, and Wouter Stol. “The Psychological and Financial Impact of Cybercrime Victimization: A Novel Application of the Shattered Assumptions Theory.” *Social Science Computer Review* 40, no. 4 (2022): 933–54. https://doi.org/10.1177/0894439320983828.

CSA Teddy Lesmana, Eva Elis, and Siti Hamimah. “Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia.” *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia*, 2022. https://doi.org/10.52005/rechten.v3i2.78.

Damasha Khoiri Clevalda. “Perlindungan Hukum Terhadap Nasabah Bank.” *Privat Law*, 2021.

Dla Piper. “Data Protection Laws Of The World: United States [Daring].” Dla Piper. Accessed November 10, 2023. Https://www.dlapiperdataprotection.com/Index.Html?T=Law&C=Us, .

Farid, Muhammad. “Penyebarluasan Informasi Mengenai Bentuk Dan Macam Tindakan Cyberbullying Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dan Upaya Pencegahannya Melalui Keb.” *Jurnal Sumbangsih*, 2020. https://doi.org/10.23960/jsh.v1i1.11.

Faude, Benjamin, and Michal Parizek. “Contested Multilateralism as Credible Signaling: How Strategic Inconsistency Can Induce Cooperation among States.” *Review of International Organizations* 16, no. 4 (2021): 843–70. https://doi.org/10.1007/s11558-020-09398-7.

Hadijan, Rusli. “‘Metode Penelitian Hukum Normatif: Bagaimana?’” *Law Review, Fakultas Hukum Universitas Pelita Harapan* 5, no. 3 (2006): 50.

Hamid, Edy Suandi. “Human Development Index and the Forming Factors: The Effect of Global Competitiveness Index in Ten ASEAN Countries.” *Journal Of International Business And Economics* 7, no. 2 (2019). https://doi.org/10.15640/jibe.v7n2a7.

Horcher, Karen A. *Essentials of Financial Risk Management*. *Essentials of Financial Risk Management*, 2005. https://doi.org/10.1002/9781118386392.

Infocomm Media Development Authority (Imda). “Singapore Gears Up For Cyber Security [Daring] Imda.” imda, 2017. Https://www.imda.gov.sg/About/Newsroom/Archived/Ida/Media Releases/2005/20050712110643.

Intan Sabrina, Mohamad, and Irma Ruslina Defi. “Telemedicine Guidelines in South East Asia—a Scoping Review.” *Frontiers in Neurology* 11 (2021): 581649.

Ismantara, S, and Y Prianto. “Relevansi Hukum Perlindungan Konsumen Indonesia Di Era Ekonomi Digital.” *Prosiding Serina*, 2022.

Jones, A., Smith, B., & Johnson, C. “Globalization and Cybercrime: The Need for International Legal Cooperation 10.” *International Journal of Cybersecurity,* (2), (2018): 145–62.

Khasanah, Nurul, and Tata Sutabri. “Analisis Kejahatan Cybercrime Pada Peretasan Dan Penyadapan Aplikasi Whatsapp.” *Blantika : Multidisciplinary Journal* 2, no. 1 (2023): 44–55. https://doi.org/10.57096/blantika.v2i1.13.

Longtchi, Theodore, Rosana Montañez Rodriguez, Laith Al-Shawaf, Adham Atyabi, and Shouhuai Xu. “Internet-Based Social Engineering Attacks, Defenses and Psychology: A Survey.” *arXiv Preprint arXiv:2203.08302*, 2022.

Malaysia, Cybersecurity. *Laporan Tahunan Cybersecurity Malaysia*. Selangor: Darul Ehsan, 2011.

Ministry Of Communications And Information. “Singapore’s Cybersecurity Strategy 2016 [Daring] Ministry Of Communications And Information.,” 2016. Https://www.csa.gov.sg/News/ Publications/Singapore-Cybersecurity-Strategy, .

Mugarura, Norman, and Emma Ssali. “Intricacies of Anti-Money Laundering and Cyber-Crimes Regulation in a Fluid Global System.” *Journal of Money Laundering Control* 24, no. 1 (2020): 10–28. https://doi.org/10.1108/JMLC-11-2019-0092.

Nguyen, Tuan Anh, Kalybek Koblandin, Shukran Suleymanova, and Vladimir Volokh. “Effects of ‘Digital’ Country’s Information Security on Political Stability.” *Journal of Cyber Security and Mobility* 11, no. 1 (2022): 29–52. https://doi.org/10.13052/jcsm2245-1439.1112.

O’connor, N. “Reforming The Us Approach To Data Protection And Privacy [Daring].” Council On Foreign Relations., 2018. Https://www.cfr.org/Report/Reforming-Us-Approach-Data-Protection, .

Onomrerhinor, Flora Alohan. “Eliminating Safe Havens for Transnational Cybercrimes in the African Continental Free Trade Area.” *Journal of Intellectual Property and Information Technology Law (JIPIT)* 2, no. 1 (2022): 49–81. https://doi.org/10.52907/jipit.v2i1.206.

Porcedda, Maria Grazia, and David S. Wall. “Modelling the Cybercrime Cascade Effect in Data Crime.” In *Proceedings - 2021 IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2021*, 161–77, 2021. https://doi.org/10.1109/EuroSPW54576.2021.00025.

Prastini, Endang. “Kebijakan Kriminal Pemerintah Terhadap Kejahatan Dunia Maya (Cyber Crime) Di Indonesia.” *Jurnal Surya Kencana Dua*, 2018.

Rowe, Brenda I. “Transnational State-Sponsored Cyber Economic Espionage: A Legal Quagmire.” *Security Journal* 33, no. 1 (2020): 63–82. https://doi.org/10.1057/s41284-019-00197-3.

Silangit, Arnold Sotarduga, Laili Furqoni, and Fanny Tanuwijaya. “Perlindungan Hukum Terhadap Korban Penganiayaan Yang Dilakukan Oleh Oknum Polri Saat Aksi Demonstrasi.” *Interdisciplinary Journal On Law, Social Sciences And Humanities*, 2022. https://doi.org/10.19184/idj.v3i1.29497.

Singapore., Personal Data Protection Commssion (Pdpc). “Who We Are [Daring] Pdpc Singapore.” Accessed November 10, 2023. Https://www.pdpc.gov.sg/About-Us/Who-We-Are, .

Situngkir, Danel Aditia. “Asas Legalitas Dalam Hukum Pidana Nasional Dan Hukum Pidana Internasional.” *Soumatera Law Review*, 2018.

Sodikov, Aziz, Zuhriddin Rizaev, Lee Chin, and Shahnoza Ochilova. “Impact of National Competitiveness on Economic Growth and Income Level – Evidence From the Selected Post-Soviet Countries.” *Research in World Economy* 12, no. 2 (2021): 17. https://doi.org/10.5430/rwe.v12n2p17.

“Studi Literatur Kejahatan Siber Pada Sistem Perbankan Syariah Di Era 4.0.” *AGHNIYA: Jurnal Ekonomi Islam* 4, no. 2 (2022). https://doi.org/10.30596/aghniya.v4i2.12759.

Sviatun, O, O Goncharuk, Chernysh Roman, Olena Kuzmenko, and Ihor V Kozych. “Combating Cybercrime: Economic and Legal Aspects.” *WSEAS Transactions on Business and Economics* 18 (2021): 751–62.

Tarigan, Ahmad Junaedy, Adil Akhyar, and Mustamam Mustamam. “Perlindungan Hukum Terhadap Korban Pornografi Dalam Media Sosial Perspektif Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik.” *Jurnal Ilmiah METADATA*, 2023. https://doi.org/10.47652/metadata.v5i1.318.

Utama, Indra. “Perlindungan Hukum Terhadap Debitur (Nasabah) Dalam Perjanjian Kredit Tanpa Agunan Ditinjau Dari Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen.” *Islamic Circle*, 2021. https://doi.org/10.56874/islamiccircle.v1i2.288.

Wahyuni, Raden Ani Eko, and Darminto Hartono. “Implementation Of Legal Protection By The Government In Order To Empowerment Of Micro Small Medium Enterprise To Realize The Justice Economy (Research Study: The Office of Cooperative and Micro Small and Medium Enterprise Province of Central Java).” *Diponegoro Law Review* 4, no. 1 (2019): 388. https://doi.org/10.14710/dilrev.4.1.2019.388-396.

Weijer, Steve van de, Rutger Leukfeldt, and Sophie Van der Zee. “Reporting Cybercrime Victimization: Determinants, Motives, and Previous Experiences.” *Policing* 43, no. 1 (2020): 17–34. https://doi.org/10.1108/PIJPSM-07-2019-0122.

cek

ORIGINALITY REPORT

25%	23%	14%	12%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	journal.unnes.ac.id Internet Source	2%
2	cfds.fisipol.ugm.ac.id Internet Source	1%
3	eudl.eu Internet Source	1%
4	proceedings.unimal.ac.id Internet Source	1%
5	Submitted to American Public University System Student Paper	1%
6	www.scilit.net Internet Source	1%
7	pure.southwales.ac.uk Internet Source	1%
8	ojs.unud.ac.id Internet Source	1%
9	Moh. Indra Bangsawan, Budi Santoso, M. Junaidi, Dewi Kusuma Diarti, Sandya	1%

	Mahendra, Engine Kubota. "Personal Data Protection Policy during Covid-19 Pandemic Era", Law and Justice, 2023 Publication	
10	ejurnalmalahayati.ac.id Internet Source	<1 %
11	ejournal.steitholabulilmi.ac.id Internet Source	<1 %
12	journal.strathmore.edu Internet Source	<1 %
13	osc.fhisip.ut.ac.id Internet Source	<1 %
14	www.jital.org Internet Source	<1 %
15	www.researchgate.net Internet Source	<1 %
16	www.grafiati.com Internet Source	<1 %
17	rechten.nusaputra.ac.id Internet Source	<1 %
18	123dok.com Internet Source	<1 %
19	ijospl.org Internet Source	<1 %

20	Submitted to Yonkers High School Student Paper	<1 %
21	discovery.researcher.life Internet Source	<1 %
22	e-journal.unipma.ac.id Internet Source	<1 %
23	Wahab Aznul Hidaya. "The Role of Witness and Victim Protection Agency for Imekko Tribe in Criminal Justice System in Sorong", Law and Justice, 2023 Publication	<1 %
24	ejournal.sidyanusa.org Internet Source	<1 %
25	journal.stihtb.ac.id Internet Source	<1 %
26	journal.uin-alauddin.ac.id Internet Source	<1 %
27	Submitted to Old Dominion University Student Paper	<1 %
28	academic.oup.com Internet Source	<1 %
29	ras.jes.su Internet Source	<1 %
30	weis2022.econinfosec.org Internet Source	<1 %

31	Submitted to Australian National University Student Paper	<1 %
32	ejournal.balitbangham.go.id Internet Source	<1 %
33	ejournal.undiksha.ac.id Internet Source	<1 %
34	Kalidasan Vasodavan, Kumitaa Theva Das. "Advancing precision medicine with gene and cell therapy in Malaysia: Ethical, Legal, and Social Implications (ELSI)", Human Gene Therapy, 2023 Publication	<1 %
35	Submitted to Keimyung University Student Paper	<1 %
36	islamicmarkets.com Internet Source	<1 %
37	ejournal.catuspata.com Internet Source	<1 %
38	journal.unismuh.ac.id Internet Source	<1 %
39	jurnal.unived.ac.id Internet Source	<1 %
40	scholars.mssm.edu Internet Source	<1 %

41	ijersc.org Internet Source	<1 %
42	journal.formosapublisher.org Internet Source	<1 %
43	www.btn.co.id Internet Source	<1 %
44	Nurul Amalia Rendreana, Setiyo Cahyono, Rheva Anindya Wijayanti. "Implementation of Gamification to Enhance Understanding of Personal Data Protection based on Republic of Indonesia Law Number 27 of 2022", 2023 International Conference on Informatics, Multimedia, Cyber and Informations System (ICIMCIS), 2023 Publication	<1 %
45	ejournal.unisba.ac.id Internet Source	<1 %
46	ijmmu.com Internet Source	<1 %
47	repository.unika.ac.id Internet Source	<1 %
48	jurnal.fh.unila.ac.id Internet Source	<1 %
49	scholarship.law.gwu.edu Internet Source	<1 %

50	siladikti.hangtuah.ac.id Internet Source	<1 %
51	ssbfnet.com Internet Source	<1 %
52	"Borneo Studies in History, Society and Culture", Springer Science and Business Media LLC, 2017 Publication	<1 %
53	Submitted to Universitas Negeri Semarang Student Paper	<1 %
54	Submitted to University of Glasgow Student Paper	<1 %
55	ijsshr.in Internet Source	<1 %
56	jurnal.umsu.ac.id Internet Source	<1 %
57	www.ijrrjournal.com Internet Source	<1 %
58	strathprints.strath.ac.uk Internet Source	<1 %
59	Ari Wibowo, Widya Alawiyah, Azriadi. "The importance of personal data protection in Indonesia's economic development", Cogent Social Sciences, 2024 Publication	<1 %

60	Submitted to Multimedia University Student Paper	<1%
61	journal.untar.ac.id Internet Source	<1%
62	Ariefulloh Ariefulloh, Hibnu Nugroho, Angkasa Angkasa, Riris Ardhanariswari. "Restorative justice-based criminal case resolution in Salatiga, Indonesia: Islamic law perspective and legal objectives", Ijtihad : Jurnal Wacana Hukum Islam dan Kemanusiaan, 2023 Publication	<1%
63	Tina Amelia, Holilur Rohman. "Formulation of Specific Personal Data Protection in Relation to Court Decisions", KnE Social Sciences, 2024 Publication	<1%
64	edepositireland.ie Internet Source	<1%
65	ejurnalriset.com Internet Source	<1%
66	online-journal.unja.ac.id Internet Source	<1%
67	talenta.usu.ac.id Internet Source	<1%
68	Hastuti, Sri Yuni. "Rekonstrksi Sistem Perlindungan Hukum Terhadap Anak Korban	<1%

Pencabulan yang Mampu Mewujudkan Keadilan", Universitas Islam Sultan Agung (Indonesia), 2023
Publication

---

69 Submitted to International Compliance Association
Student Paper
<1%

---

70 Nathalina Naibaho, Yosefin Mulyaningtyas. "Chapter 9 Victim Protection of Multiple Victimization of Violence in Indonesia: A Right Way to Go?", Springer Science and Business Media LLC, 2022
Publication
<1%

---

71 Nofie Iman. "chapter 2 Regulating Digital Platforms", IGI Global, 2021
Publication
<1%

---

72 Novrianti Novri, Florianus Yudhi Priyo Amboro, Rufinus Hotmaulana Hutauruk. "A Analisis Perlindungan Konsumen dalam Tindakan Penyalahgunaan Data Pribadi oleh Penyelenggara Pinjaman Online Berdasarkan Perspektif Hukum Indonesia", AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam, 2023
Publication
<1%

---

73 Yulia Kusuma Wardani, Torkis Lumban Tobing, Putri Ariyanti, Depri Liber Sonata, Dianne Eka Rusmawati. "ANTICIPATING FINANCIAL AND DATA PRIVACY RISK: ASSESSING LEGAL
<1%

RIGHTS AND RESPONSIBILITIES IN ONLINE SOCIAL GATHERING IN INDONESIA", Indonesia Private Law Review, 2023
Publication

74	brill.com Internet Source	<1 %
75	buletinhukum.com Internet Source	<1 %
76	s899a9742c3d83292.jimcontent.com Internet Source	<1 %
77	thebabe.stiebankbpdjateng.ac.id Internet Source	<1 %
78	"Proceedings of Eighth International Congress on Information and Communication Technology", Springer Science and Business Media LLC, 2023 Publication	<1 %
79	Agnes Fitryantica, Regy Hermawan. "Fast-Track Legislation Mechanism as an Alternative to the Formation of Legislation in Indonesia", Jurnal Ilmiah Kebijakan Hukum, 2022 Publication	<1 %
80	Alexandra Florecita Adja Mossa. "Criminal Liability Policy Of Persons With Mental Disorders In Case Spreading Racial Issues", Ius Poenale, 2022 Publication	<1 %

81	Submitted to University of Wales Swansea Student Paper	<1 %
82	ejournal.umm.ac.id Internet Source	<1 %
83	indonesia.iom.int Internet Source	<1 %
84	journal.mengeja.id Internet Source	<1 %
85	jurnal.unsur.ac.id Internet Source	<1 %
86	ojs.uninus.ac.id Internet Source	<1 %
87	papers.academic-conferences.org Internet Source	<1 %
88	www.asianinstituteofresearch.org Internet Source	<1 %
89	www.ijems.id Internet Source	<1 %
90	www.unescap.org Internet Source	<1 %
91	Brierly Napitupulu. "SUPREME COURT DECISIONS ON PUBLIC INFORMATION AND PERSONAL DATA PROTECTION", Indonesia Private Law Review, 2022 Publication	<1 %

92	Pavol Sokol, Radoslav Benko, Laura Rózenfeldová. "Chapter 13 Legal Issues of Deception Systems in the Industrial Control Systems", Springer Science and Business Media LLC, 2020 Publication	<1 %
93	Septhian Eka Adiyatma. "Legal Paradox: Protection of Victims Taking the Law into Vigilantism", Ius Poenale, 2023 Publication	<1 %
94	Jelena Matijasevic-Obradovic. "European standards in the field of combating cyber crime", Megatrend revija, 2014 Publication	<1 %
95	Nur Amalina Putri Adytia, Syarif Zakaria Said Wachdin, Said Said. "The Legal Framework for Personal Data Protection in the Digital Era as Fulfillment of Privacy Rights in Indonesia", KnE Social Sciences, 2024 Publication	<1 %
96	Salwa Salsabilla, Imran Bukhari Razif, Ulil Albab. "Legal Protection Against Sexual Violence on Women: A Study on Legislation", SIGn Jurnal Hukum, 2023 Publication	<1 %
97	Zaka Firma Aditya, Sholahuddin Al-Fatih. "Indonesian constitutional rights: expressing	<1 %

and purposing opinions on the internet", The International Journal of Human Rights, 2020
Publication

98	newinera.com Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		