STRENGTHENING INDONESIA'S EIT LAW TO COMBAT RANSOMWARE THREATS: A LEGAL FRAMEWORK ANALYSIS

Muhammad Alpajri
Master of Law Study Program, University of Riau
E-mail: muhammad.alpajri7858@grad.unri.ac.id

Erdianto
Faculty of Law, University of Riau
Email: erdianto.effendi@lecturer.unri.ac.id

Davit Rahmadan
Faculty of Law, University of Riau
Email: davitrahmadan@lecturer.unri.ac.id

Abstract

Ransomware is a type of malware designed to lock or encrypt victim data so that it cannot be accessed. Once the victim's data is locked, the perpetrator will ask for a ransom to restore access, usually in the form of digital currency such as Bitcoin which is difficult to track. Ransomware crimes are regulated in Article 33 of the ITE Law, however, Article 33 of the Electronic Information and Transactions Law (UU ITE) has weaknesses in its formulation because it does not include specific elements related to ransomware crimes, especially in relation to the element of requesting ransom payments. This creates a lack of legal certainty regarding ransomware crimes so that many cases of ransomware crimes cannot be prosecuted due to legal gaps. The purpose of this study is to provide input to law enforcement, police, prosecutors, judges, and the community and government in Countering the Threat of Ransomware Crimes in Indonesia. Based on the results of the study and discussion, it can be concluded. First, Article 33 of the Electronic Information and Transactions Law only regulates disruption of electronic systems, but does not explicitly include the elements of "extortion" or "demand for ransom payment" which are the core of ransomware crimes. Second, to strengthen the Electronic Information and Transactions Law and Indonesia's legal framework in countering the threat of ransomware, several important steps must be taken. First, one of the main solutions in dealing with ransomware crimes is to add provisions that explicitly regulate this crime in legislation, especially in the Electronic Information and Transactions Law.

Keywords: Information and Electronic Transactions Law, Ransomware Crime, Indonesia

I. INTRODUCTION

Ransomware is a type of malware designed to lock or encrypt a victim's data so that it cannot be accessed. Once the victim's data is locked, the perpetrator will demand a ransom to restore access, usually in the form of a digital currency such as Bitcoin that is difficult to trace . [1]Ransomware attacks can spread through a variety of methods, including phishing emails, infected software [2]downloads , or through vulnerabilities in network systems.

The crime of ransomware can be categorized under the ITE Law as a crime

[1] https://www.linknet.id/article/ransomware/ accessed on July 18, 2024, at 09.35 WIB .

[2] https://www.detik.com/jogja/berita/d-7407523/apa-itu-ransomware-ini-bahaya-mekanisme-cara-mengatasi-sample-casenya/ accessed on July 18, 2024, at 09.35 WIB .

regulated in Article 33 of the ITE Law which reads:

> "Any person who intentionally and without rights or unlawfully carries out any action that results in disruption of the Electronic System and/or causes the Electronic System to not work as it should"

However, Article 33 of the Electronic Information and Transactions Law (UU ITE) has weaknesses in its formulation because it does not include specific elements related to ransomware crimes, especially in relation to the element of requesting ransom payments. Ransomware itself is a form of cybercrime in which malicious software is used to encrypt data or lock access to a computer system until the victim pays a certain amount of money as a ransom in order to regain access. In this crime, the main element that must be considered is the existence of coercive actions against the victim to pay a ransom as a condition for reopening access to data that has been locked or encrypted by the perpetrator.

If examined further, Article 33 of the Electronic Information and Transactions Law only regulates disruption of electronic systems, but does not explicitly include the elements of "extortion" or "demand for ransom payment" which are the core of ransomware crimes. The formulation of light sanctions in the article is also a weakness, because it does not provide a sufficient deterrent effect for cybercriminals who use ransomware as a modus operandi. In the context of criminal law, the principle of legality as regulated in Article 1 paragraph (1) of the Criminal Code (KUHP) states that an act cannot be punished if there are no regulations that clearly regulate and prohibit the act. Therefore, Article 33 of the ITE Law which does not specifically include the element of demand for ransom payment has the potential to conflict with the principle of legality, because it can create ambiguity in its application to ransomware cases.

In addition, the principle of legality in criminal law also requires that criminal regulations must be formulated clearly and must not be open to multiple interpretations so that there is no legal uncertainty for the community. In this case, the inaccuracy of the formulation of Article 33 of the Electronic Information and Transactions Law can result in legal loopholes that can be exploited by ransomware perpetrators to avoid legal entanglement or receive punishments that are not commensurate with the impacts caused. Thus, it is necessary to revise existing regulations or add new articles that specifically regulate ransomware crimes, including the element of requesting ransom payments, to be in line with the principle of legality and ensure legal certainty in enforcing the law against this cybercrime.

Strengthening the Electronic Transactions Law on Electronic Systems and Electronic Documents, especially the provisions of substantive law, is needed to deal with increasingly complex ransomware . The addition of special ransomware offenses will provide a clear legal basis for dealing with data

hostage taking, unauthorized encryption, and digital extortion. Stricter and more proportionate sanctions can be applied, especially when attacks have a wide impact or target critical sectors such as government infrastructure, health, or finance. preventing and handling ransomware attacks .[3]

Based on the background and problems, the author is interested in discussing research with the title "Strengthening Indonesia's Eit Law To Combat Ransomware Threats: A Legal Framework Analysis"

II. RESEARCH METHODS

This type of research is classified as normative legal research of the legal synchronization type . Legal synchronization is the alignment of how far a particular legal system is aligned vertically, namely based on the hierarchy of legal regulations, or horizontally, namely equal legal regulations.[4]

However, if seen from its nature, the research is descriptive, namely research that is aimed at producing data that is as detailed and sufficient as possible about humans, conditions or other symptoms, and only elaborates on the conditions of the problematic object without intending to create valid conclusions. general.[5]

III. RESULTS AND DISCUSSION

3.2 Regulation of Ransomware Criminal Acts in the Electronic Information and Transactions Law

Ransomware in Indonesia has entered a worrying stage in early 2024 alone, Indonesia has experienced many ransomware- based cyber attacks , one example that is currently viral is where the Temporary National Data Center Server (PDNS) has experienced a Ransomware attack since Thursday, June 20, 2024, causing 210 government agencies to be affected and digital-based public services to be disrupted. The latest type of ransomware cyber attack Brain Cipher to the National Data Center Meanwhile, the perpetrators of the cyber crime asked for a ransom from the PDNS manager, namely Telkomsigma and the Ministry of Communication and Information (Kemenkominfo) of US$ 8 million or equivalent to IDR 131 billion. [6]What's sad about the Ransomware -Based Cyber Attack that attacked the Temporary National Data Center Server (PDNS), the government was not ready for this so that only 2 percent of the Temporary National Data Center Server (PDNS) data could be backed up by the Ministry of Communication and Information .[7]

[3]Dilla Ayuna Letri , et.al, Legal Protection for Victims in Cyber Sabotage Cases and Extortion According to Positive Law in Indonesia, *Rio Law Journal Volume . 4 Number . 2, December 2023, Faculty of Law,* Ekasakti University , p. 401.

[4] Soerjono Soekanto , *Introduction to Legal Research* , 1981, UI Press, Jakarta, p. 43.

[5] Soerjono Soekanto , *Introduction to Legal Research* , 1981, UI Press, Jakarta, p. 43.

[6]https://techno.okezone.com/read/2024/06/24/54/3025387/tengah-data-nasional-diserang-ransomware-pelaku-minta-tebusan-rp131-triliun?page=all/ accessed on July 18, 2024, 08.24 WIB .

[7]https://tirto.id/ kepala- bssn-hanya-2-data-ter-backup-saat-diserang-ransomware-gZ5l / accessed on July 18, 2024, 08.39 WIB .

The large number of ransomware cases in Indonesia is caused by weaknesses in the regulations of the Republic of Indonesia Law Number 19 of 2016, which amended Law Number 11 of 2008 concerning Electronic Information and Transactions and was revised again through Law Number 1 of 2024 concerning Electronic Information and Transactions which is the legal umbrella for cybercrime in Indonesia is unable to answer the problem of Ransomware Crimes in Indonesia, the reference for Ransomware Crimes is Article 33 of the ITE Law which reads:

> "Any person who intentionally and without rights or unlawfully carries out any action that results in disruption of the Electronic System and/or causes the Electronic System to not work as it should"

However, Article 33 has a weakness in its formulation because it does not cover specific elements related to ransomware crimes, especially in relation to the element of requesting ransom payments, this causes Article 33 of the ITE Law to conflict with the principle of legality put forward by Paul Johan Anselm Ritter von Feuerbach. This principle of legality is known as the adage " Nullum delictum nulla poena sine praevia lege poenali " which means that there is no crime (delict) and no punishment without previously established legal rules. This principle is the main foundation in criminal law which aims to ensure legal certainty and prevent abuse of power in the law enforcement process. Thus, every act that can be subject to criminal sanctions must be clearly regulated in previously applicable laws and regulations.

This adage is divided into three main parts, each of which emphasizes a basic principle in criminal law.

1) First, Nulla poena sine lege, which means there is no punishment without a statutory provision. This emphasizes that an act can only be punished if it has been explicitly regulated in the applicable legal regulations.
2) Second, Nulla poena sine crimine, which states that there is no punishment without a criminal act. This means that a person cannot be sentenced if he is not proven to have committed an act that is categorized as a criminal act.
3) Third, Nullum crimen sine poena legali, which means there is no criminal act if there is no provision for punishment regulated by law.

This principle ensures that an act can only be categorized as a crime if it has been expressly determined in the applicable legal regulations. Based on these principles, the weakness of Article 33 of the Electronic Information and Transactions Law can arise if the article does not strictly fulfill the principle of legality. If the norms in this article are formulated vaguely or open to multiple interpretations, then there is a potential violation of the principle of legality because it opens up opportunities for arbitrary law enforcement.

This can result in legal uncertainty for the community and the perpetrators accused of violating the article. Therefore, in the application of criminal law, especially those related to information technology and electronic transactions, clarity of norms is very important to comply with the principle of Nullum delictum nulla poena sine praevia lege poenali which is the main pillar in the modern criminal law system.

Then, according to Jeschek and Weigend's opinion, as quoted by Machteld Boot (2001), it is emphasized that the principle of legality in criminal law contains three main principles.

1) First, the Lex Scripta Principle, which means that the formulation of criminal law rules must be written. This principle emphasizes that criminal law norms must not be based on unwritten legal customs or practices, thus ensuring legal certainty and avoiding subjective application of law.
2) Second, the Lex Certa Principle, which requires the formulation of criminal law to be clear and not open to multiple interpretations. This means that a criminal law rule must be formulated in clear language, so as not to cause ambiguity in its application.
3) The principle of Lex Stricta, which emphasizes that criminal law rules must be formulated strictly and prohibits the use of analogies in criminal law. This principle aims to avoid overly broad or flexible interpretations of the law, which could potentially harm individuals by unlawfully expanding the scope of criminalization.

Based on these principles, weaknesses can be seen in the formulation of Article 33 of the Electronic Information and Transactions Law, especially in terms of the unclear elements of the act or object related to the phrase "asking for ransom payment". This ambiguity has the potential to give rise to different interpretations in law enforcement practices, which are contrary to the principle of Lex Certa. The criminal law norms in the article should specifically describe actions that are categorized as criminal acts, including how the element of "asking for ransom payment" must be proven legally. In addition, the weak formulation of sanctions in this article also creates a loophole that can reduce the deterrent effect on perpetrators of cybercrime.

Ransomware crime, as explained by experts, this crime involves the use of malicious software that locks the keyboard or computer to prevent access to data until the victim pays a certain amount of money as a ransom. However, if Article 33 of the ITE Law does not explicitly accommodate the elements that form the crime of ransomware, then its application could be difficult and potentially inconsistent with the principle of legality in criminal law.

The next weakness in Article 33 of the ITE Law is the light criminal threat given, even though the criminal act regulated has a very

large impact. This article stipulates that anyone who meets the elements as referred to in the article can be punished with a maximum imprisonment of 10 years and/or a maximum fine of IDR 10,000,000,000.00 (ten billion rupiah). When compared to the level of danger posed by cybercrime, especially ransomware crimes, this criminal threat is considered insufficient to provide a deterrent effect for the perpetrators. In many cases, ransomware attacks can cause economic losses that are much greater than the fines regulated in the article, even reaching hundreds of billions of rupiah on a wider scale.

Ransomware crimes is not only limited to the financial aspect, but can also threaten data security, harm companies, and endanger important sectors such as health, government, and critical infrastructure. For example, ransomware attacks targeting hospitals or government systems can cause disruptions to public services that result in major losses for the community. In addition, cyber attacks that successfully break into large corporate systems can result in large amounts of customer data being leaked, which can then potentially be used for other crimes, such as identity theft and online fraud.

3.2 Strengthening the Electronic Information and Transactions Law in Countering the Threat of Ransomware Crimes in Indonesia

Strengthening the Electronic Information and Transactions Law in countering the threat of ransomware crime requires updating and strengthening regulations that are more focused and relevant to the challenges of modern cybercrime. The Electronic Information and Transactions Law needs to be strengthened in several key aspects to be more relevant and responsive to technological developments and cybercrime patterns.

1. Adding Provisions That Explicitly Regulate Ransomware Crimes In Legislation

   Clarity of regulation is essential to avoid multiple interpretations in law enforcement and so that perpetrators can be prosecuted under the appropriate articles. Currently, Article 33 of the Electronic Information and Transactions Law still does not cover the main elements of ransomware, namely the demand for ransom payment as a condition for reopening access to data that has been locked or encrypted.

   With more specific regulations, any act of digital extortion involving the use of malicious software can be clearly categorized as a criminal act with sanctions appropriate to the level of crime committed.

2. The Electronic Information and Transactions Law Must Include Obligations for Public and Private Organizations to Implement Cybersecurity Standards

   The Electronic Information and Transactions Law should also include a requirement to conduct regular cybersecurity audits. These audits aim to identify weaknesses in an organization's

security systems and procedures before they are exploited by ransomware actors.

Security audits should include a review of access protocols, data usage policies, and cyberattack readiness. With scheduled and standardized audits, organizations can not only detect potential threats but also fix deficiencies before an incident occurs.

3. Electronic Information and Transactions Law Needs to be More Comprehensively Integrated with Personal Data Protection Law

This integration could set up an obligation for organizations to report ransomware attacks to authorities and provide notification to individuals whose data has been compromised. This would help victims take further protective measures, such as changing passwords or monitoring suspicious activity on their accounts.

In addition, in the integration of the Electronic Information and Transactions Law and the Personal Data Protection Law, provisions can be added that regulate the mechanism for handling and recovering data after a ransomware attack.

4. Tightening Criminal Sanctions for Ransomware Perpetrators

Tighten criminal penalties for ransomware perpetrators, especially for attacks targeting critical infrastructure, the health sector, or government agencies. Given the huge impact that ransomware attacks have on these vital sectors, stricter penalties will provide a stronger deterrent effect and emphasize the government's seriousness in dealing with the threat of cybercrime.

Another strategic step is the formation of a special unit that specifically handles cybercrime, including ransomware, within institutions such as the police and prosecutors. This unit can be staffed by personnel with high technical skills who focus on handling cyber cases, from investigation to prosecution. With a special unit, ransomware cases can be handled more effectively and efficiently, because this unit can fully concentrate on the unique challenges faced in cybercrime, without being distracted by assignments in other areas.

The combination of increasing technical capacity and establishing a special unit will enable Indonesia to be better prepared to deal with ransomware threats. This will not only strengthen the ability to enforce the law, but also send a strong signal that cybercrime will not be left unpunished without serious consequences. This effort can also improve cooperation with the international community, which is crucial in dealing with transnational ransomware crimes.

International cooperation is an important element in dealing with ransomware threats that often involve transnational actors. In many cases,

ransomware attacks are carried out by groups or individuals operating from other countries, utilizing global networks, anonymous technology, and sophisticated infrastructure that are difficult to track. Therefore, Indonesia needs to strengthen cooperation with various parties, both through bilateral agreements with other countries and multilateral partnerships with international organizations such as Interpol, Europol, and agencies that focus on cybersecurity. This cooperation allows Indonesia to gain access to a global information network that can help track ransomware criminals to their source.

Through international collaboration, Indonesia can share intelligence data related to ransomware attacks, including the methods used by perpetrators, attack patterns, and tools used to encrypt victim data. This information can be used to accelerate the identification of perpetrators and understand broader criminal networks. In addition, this collaboration also opens up opportunities for Indonesia to utilize advanced technologies, such as digital forensic analysis tools and cryptocurrency transaction tracking tools, which are often used as ransom payments in ransomware cases. By accessing this technology, law enforcement can trace digital transactions to the parties involved in the crime.

International cooperation also provides an opportunity for Indonesia to participate in global operations designed to dismantle ransomware crime networks. Such operations usually involve a number of countries sharing information and resources to catch the perpetrators and stop their activities. In addition, Indonesia can learn from the best practices of other countries that have successfully handled ransomware effectively, both through policies, technology, and legal strategies implemented.

Moreover, international cooperation also includes strengthening legal diplomacy, such as accelerating the extradition process for perpetrators caught in other countries, as well as ensuring the harmonization of cross-country regulations to facilitate law enforcement. With an active commitment to global cooperation, Indonesia can demonstrate its seriousness in protecting its digital infrastructure, while contributing to international efforts to create a safer digital ecosystem. This kind of cooperation will not only improve the country's ability to ward off ransomware but also strengthen Indonesia's position as a strategic partner in global cybersecurity.

Ransomware crimes is to add provisions that explicitly regulate this crime in legislation, especially in the Electronic Information and Transactions Law . Clarity of regulation is very necessary so that there is no multi-interpretation in law enforcement and so that perpetrators can be charged with the appropriate article. Currently, Article 33 of the Electronic

Information and Transactions Law still does not cover the main element in ransomware, namely the request for ransom payment as a condition for reopening access to data that has been locked or encrypted.

With more specific regulations, any act of digital extortion involving the use of malicious software can be clearly categorized as a criminal act with sanctions appropriate to the level of crime committed. In addition, strengthening regulations is needed in the form of increasing the threat of sanctions for cybercriminals, especially those that have a broad impact on individuals, companies, and public infrastructure. Ransomware crimes not only cause huge financial losses, but can also threaten national security if the attacked system is part of critical infrastructure, such as health services, government, or energy.

Therefore, the punishment given to the perpetrator must be heavier and proportional to the level of loss caused. If the criminal threat given is too light, then this can encourage the perpetrator to continue their actions because they feel the risks faced are not comparable to the benefits obtained.

This increase in penalties also needs to be accompanied by more comprehensive prevention efforts, including strengthening cooperation between the government, the private sector, and the community in dealing with cybercrime. The government needs to strengthen the capacity of law enforcement officers in handling digital crime, both through special training, development of digital forensic technology, and international cooperation in handling ransomware attacks that are often global in scale. On the other hand, companies and individuals also need to be encouraged to improve the security of their systems to reduce the risk of becoming victims of cyber attacks.

With the special regulation on ransomware in the Electronic Information and Transactions Law, legal certainty can be more assured. Law enforcement officers will also have a stronger legal basis and more effective tools to handle ransomware cases. This regulation not only protects victims but also sends a strong message to perpetrators that ransomware crimes will be dealt with firmly. This also encourages the creation of a safer and more trusted digital ecosystem in Indonesia.

IV. CONCLUSION

1. Article 33 of the Electronic Information and Transactions Law only regulates disruption to electronic systems, but does not explicitly include the elements of "extortion" or "demand for ransom payment" which are the core of ransomware crimes, so that the current Electronic Information and Transactions Law is still not responsive enough in dealing with ransomware threats because it does not have specific regulations regarding this

cyber attack. Without adequate updates and improvements, law enforcement will have difficulty in dealing with the increasingly growing ransomware crime.

2. To strengthen the Electronic Information and Transactions Law and Indonesia's legal framework in combating ransomware threats, several important steps must be taken. First, One of the main solutions in dealing with ransomware crimes is to add provisions that explicitly regulate this crime in legislation, especially in the Electronic Information and Transactions Law. Second, the implementation of obligations for public and private organizations to follow cybersecurity standards, such as the use of encryption and regular system updates, to prevent ransomware attacks. Third, the integration of the Electronic Information and Transactions Law with the Personal Data Protection Law to ensure better protection of personal data. Fourth, increasing the capacity of law enforcement by providing technical training on cybercrime and the establishment of a special unit that focuses on handling ransomware. Fifth, international and inter-agency cooperation to improve coordination in dealing with perpetrators who operate across countries. Finally, a preventive approach through educational campaigns and incentives for companies that improve their digital security. With these steps, Indonesia can strengthen its regulations and infrastructure to deal with ransomware threats more effectively and comprehensively.

BIBLIOGRAPHY

1. Book

Ahmad Rifai, Penemuan Hukum 0leh Hakim Dalam Persfektif Hukum Progresif, Jakarta: Sinar Grafika, 2011.

Amir Ilyas, Asas-Asas Hukum Pidana, Yogyakarta: Rangkang Education Yogyakarta & PuKAPIndonesia, 2012.

Antonio Cassese, International Criminal Law, University Press, Oxford: Oxford. 2013,

Badan Siber dan Sandi Negara Republik Indonesia, Lanskap Keamanan Siber Indonesia 2023, Direktorat Operasi Keamanan Siber. 2003.

Brian Krebs, Spam Nation: The Inside Story of Organized Cybercrime, Sourcebooks. 2014.

Damask, Perkembangan Hukum Pidana Kontemporer, Jakarta: Rajawali Press, 2016.

Danielle Keats Citron, Hate Crimes in Cyberspace, Harvard University Press. 2014

Darrel Menthe, Jurisdiction in Cyberspace: A Theory of the Uploader and the Downloader, Harvard Law Review. 2002.

David S. Wall, Cybercrime: The Transformation of Crime in the Information Age, Polity Press. 2007.

Hartomo, Penyidik dan Penegakan Hukum melalui Pendekatan Hukum Progresif. Jakarta: Sinar Grafika, 2010.

Ilhami Bisri, Sistem Hukum Indonesia (Cet. II; Jakarta: PT Raja Grafindo Persada, 2005.

International Meeting of Experts on The Use of Criminal Sanction in The Protection of Environment, 1994, Proceedings (Portland, Oregon: Environmental Law Institute.

Interpol, Cybercrime Strategy and Global Cooperation, (Lyon: Interpol. 2020.

Jonathan Clough, Principles of Cybercrime, Cambridge University Press. 2015.

Julia Hörnle, Cross-Border Internet Dispute Resolution, Cambridge University Press. 2009.

Soerjono Soekanto, Pengantar Penelitian Hukum, 1981, UI Press, Jakarta.

2. Regulations

Undang-Undang Dasar 1945.

Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Undang-Undang Republik Indonesi Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor I1 Tahun 2008 tentang Informasi Dan Transaksi Elektronik.

3. Journal

Agung Wiranata, "Analogi Sistem Perlindungan Hal Atas Data Pribadi Antara Indonesia Dengan Singapura", Jurnal Ilmiah Mahasiswa Hukum, Vol 3, Universitas Muhammdiyah Sumatera Utara, 2021.

Agus Rahardjo, "Karakteristik Kejahatan Siber dan Tantangan Penegakan Hukumnya," Jurnal Hukum & Teknologi, Vol. 4, No. 2 (2021).

Agus Rahardjo, "Strategi Nasional dalam Menangani Kejahatan Siber," Jurnal Hukum & Teknologi, Volume. 3, Nomor. 2 tahun 2022.

Aliya Putri Novita, Cybersecurity Threats; Analisis Dan Mitigasi Resiko Ransomwaredi Indonesia, Jurnal Simasi : Jurnal Ilmiah Sistem Informasi, Vol. 3, No. 1, Juni 2023, Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Bung Karno.

Anisa Nur Padilah dan Dinie Anggraeni Dewi, "Pancasila di Era Globalisasi dalam Memperkuat Moral untuk Membangun dan Memajukan Bangsa," Antropocene : Jurnal Penelitian Ilmu Humaniora, (November, 2021).

Arisandy, Yogi Oktafian. "Penegakan Hukum terhadap Cyber Crime Hacker." Indonesian Journal of Criminal Law and Criminology (IJCLC) 1.3, Vol 1, No 3 (2020), Fakultas Hukum, Universitas Muhammadiyah Yogyakarta.

Badan Siber dan Sandi Negara Republik Indonesia, 2003, Lanskap Keamanan Siber Indonesia 2023, Direktorat Operasi Keamanan Siber.

Bambang Widodo, "Cybercrime: Ancaman Baru di Era Digital," Jurnal Keamanan Siber Indonesia, Volume. 5, Nomor. 1 tahun 2021.

Dilla Ayuna Letri, et.al, Perlindungan Hukum Terhadap Korban Pada Kasus Cyber Sabotage and Extortation Menurut Hukum Positif di Indonesia, Rio Law Jurnal Volume. 4 Nomor. 2, Desember 2023, Fakultas Hukum Universitas Ekasakti.

Ervina Chintia, et al, Kasus Kejahatan Siber Paling Banyak Terjadi di Indonesia dan Penanganannya, Journal Information Engineering and Educational Technology, Volume 02 Nomor 02, 2018.

Russel Butarbutar, Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya, Technology and Economics Law Journal Volume 2 Nomor 2, Fakultas Hukum Universitas Bung Karno.

4. Website

https://www.lekatnews.com/2020/02/belum-tuntas-pelunasan-ganti-rugi-lahan.html accessed on 10 November 2020

https://www.linknet.id/article/ransomware/ diakases tanggal 18 Juli 2024, jam 09.35 Wib.

https://www.detik.com/jogja/berita/d-7407523/apa-itu-ransomware-ini-bahaya-mekanisme-cara-mengatasi-contoh-kasusnya/ diakases tanggal 18 Juli 2024, jam 09.35 Wib.

https://www.bssn.go.id/monitoring-keamanan-siber-2023/ diakases tanggal 19 Juli 2024, Jam 07.00 Wib.

https://www.bssn.go.id/monitoring-keamanan-siber-2023/ diakases tanggal 19 Juli 2024, Jam 07.00 Wib.

https://www.ojk.go.id/ojk-institute/id/capacitybuilding/upcoming/4021/strategi-mencegah-serangan-siber/ diakases tanggal 18 Juli 2024, Jam 07.00 Wib.

https://kominfo.lhokseumawekota.go.id/berita/read/29-juta-serangan-siber-diblokir-di-indonesia-selama-2023-/ diakases tanggal 18 Juli 2024, Jam 07.00 Wib.

https://techno.okezone.com/read/2024/06/24/54/3025387/pusat-data-nasional-diserang-ransomware-pelaku-minta-tebusan-rp131-triliun?page=all/ diakases tanggal 18 Juli 2024, Jam 08.24 Wib

https://tirto.id/kepala-bssn-hanya-2-data-ter-backup-saat-diserang-ransomware-gZ5l/ diakases tanggal 18 Juli 2024, Jam 08.39 Wib.

https://aptika.kominfo.go.id/2023/12/perubahan-kedua-atas-uu-ite-wujudkan-kepastian-hukum-ruang-digital/ diakases tanggal 22 November 2024 Jam 23.00 Wib

https://akarberita.com/ransomware-dan-keamanan-data-nasional-perspektif-hukum-ite-dalam-menghadapi-ancaman-siber/ diakases tanggal 22 November 2024 Jam 21.00 Wib

https://www.hukumonline.com/berita/a/3-poin-penting-yang-diatur-dalam-uu-ite-baru-lt65b9026e8a521/ diakases tanggal 22 November 2024 Jam 20.00 Wib

https://www.hukumonline.com/klinik/a/bunyi-pasal-30-ayat-1-uu-ite-tentang-peretasan-lt659e7c363776f/ diakases tanggal 22 November 2024 Jam 11.00 Wib

https://safenet.or.id/id/2021/03/revisi-uu-ite-total-sebagai-solusi/ diakases tanggal 22 November 2024 Jam 12.00 Wib.