Guaranteed Legal Protection for Malware Victims in Indonesia

Dhani Kristianto[1], Azis Budianto[2]

{dhanikristianto.tp94@gmail.com[1], azis_budianto@borobudur.ac.id[2]}

Universitas Borobudur[1, 2]

Abstract. The Indonesian government's efforts to provide guaranteed legal protection to the public are by Article 27 of Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE). Article 27 of the ITE Law is a critical legal basis for regulating protection against electronic transactions and cybercrimes in Indonesia. In realizing this guarantee of legal protection, the government is faced with various obstacles such as limited resources, technological complexity, cross-regional and international cooperation, protection of personal data, suboptimal understanding of the law, commercial interests as well as legal and ethical challenges. To overcome these obstacles, strategic steps are required, such as increasing the effectiveness of law enforcement, educating the public about cyber security, cross-sector collaboration, and regular regulatory evaluation. The implementation of these steps is expected to improve cyber security, protect individual rights, and ensure the continued use of information technology in Indonesia. In this way, people can feel safer and more protected when making online transactions. The government needs to continue making efforts to maintain cyber security, enforce the law fairly, and ensure that the guarantee of legal protection by Article 27 of the ITE Law can be implemented effectively for the common good.

Keywords: Guarantee, Legal protection, Malware, ITE Law.

1 Introduction

In the increasingly advanced digital era, cyber security threats such as malware have become one of the main challenges faced by people throughout the world, including in Indonesia. The consequence of malware attacks not only results in material losses but can also damage people's reputations, privacy, and information security. Therefore, guaranteeing legal protection for malware victims is significant to handle and prevent the negative impacts caused by this cyberattack.

In Indonesia, the rapid growth of internet users has opened the door to an increase in malware attacks targeting individuals and organizations. Indonesia's increasingly digitally connected society is vulnerable to malware attacks that can damage their devices, steal personal data, or even cause significant financial loss. Therefore, adequate legal protection is key in protecting the public from this malware threat. However, currently, there is still a void in guaranteeing legal protection for malware victims in Indonesia. A legal system that has not yet fully adapted to developments in information technology and cyber security needs means that people often find it difficult to obtain justice and recovery for the losses they experience due to

ICLSSEE 2024, May 25, Jakarta, Indonesia

DOI 10.4108/eai.25-5-2024.2349181

malware attacks. Apart from that, low public awareness of the importance of cyber security is also a factor that worsens this situation. Many individuals do not understand the risks associated with malware attacks, so they tend to be less vigilant in using digital technology. Broader and more effective educational efforts are needed to increase public awareness about malware threats and the preventive measures they can take. In this context, this article aims to outline the importance of guaranteeing legal protection for people who are victims of malware in Indonesia. Through an in-depth understanding of the legal issues related to malware attacks, it is hoped that concrete steps can be identified that can be taken to increase legal protection for society and reduce the negative impact of these cyberattacks.

With the guarantee of strong legal protection, it is hoped that the Indonesian people can feel safer and more protected in using digital technology, and can be more confident in facing increasingly complex and detrimental malware threats. Thus, legal politics is a choice regarding the laws that are enforced as well as choices regarding laws that will be repealed or not implemented, all of which are intended to achieve the State's objectives as stated in the Preamble to the 1945 Constitution.[1]

Law is the will of the ruler, this is in accordance with what Lili Rasyidi and Ira Rasyidi explained, quoted from Legal and Political Relations in the Indonesian Legal System), in the sense of orders from those who have the highest power or who hold sovereignty. The debate regarding the relationship between law and politics has long historical roots in legal science. For legal positivists such as John Austin, law is nothing other than a product of politics or power. On the other hand, a different view comes from the historical school of law, which sees law not from legal dogmatics and laws alone, but from the social reality that exists in society and holds the view that law depends on general acceptance in society and every groups create living laws.[2] According to Hikmahanto Juwana's analysis of Indonesia's economic laws, legal politics can be divided into two dimensions. The first pertains to the fundamental motivation for enacting legislative regulations, while the second involves the goals or underlying reasons that drive the enactment of statutory regulations.[3]

Ransomware and Malware crimes do not only attack developed countries such as America and the European Union. Indonesia itself is a country that is prone to ransomware attacks, especially those that attack data belonging to the government, state-owned companies, and the private sector. As a result, administrative services can be disrupted and have to be done manually, thus prolonging the registration process in all population and government systems[4].

How it works, Ransomware and Malware attacks occur where hackers send emails to potential victims containing certain links. When the link is clicked, the malicious program automatically works to encrypt folders, files and even drives on the computer. Even if the user or victim cleans their computer from viruses, the encrypted files, folders, or drives still cannot be used again without the hacker holding the key.[5]. Indonesian people are too lazy to read, the high interest of Indonesian people in sensational news, the curiosity gap (a gap that makes curious readers click on links to answer their curiosity), and the information gap (readers want to get clarity and reduce uncertainty) cause Indonesian people to easy to fall for clickbait. Apart from that, the existence of business competition between online news producers has caused many online media to use this technique to increase their site traffic[6].

The American government is currently still at the stage of debate as to whether clickbait needs to be regulated in the form of a regulation or whether it does not require special regulations to regulate it. The Ministry of Communication and Information as a regulator in Indonesia

carries out blocking actions on negative content such as content related to terrorism, content that spreads hatred associated with ethnicity, religion, race, and inter-group (SARA), hoaxes, pornography, has not seen the need to make special regulations on clickbait content. Therefore, in Indonesia until now no regulation specifically regulates clickbait, even though it has been found that more than 50 percent of internet users are trapped and interested in clicking on clickbait articles and opening links sent by strangers, even though there is a possibility of infiltrated by malware, viruses, or there is data theft risk.[7].

In Indonesia, regulations regarding malware are regulated in various laws and regulations which aim to protect the public from the threat of cyberattacks. Several necessary regulations related to handling malware in Indonesia include:

1. Electronic Information and Transactions Law (UU ITE).

   The ITE Law is a law that is the legal basis for electronic transactions in Indonesia. In the context of malware, the ITE Law regulates computer crimes, including the spread of harmful malware. The articles in the ITE Law provide the legal basis for law enforcement against perpetrators of computer crimes, including those related to malware.

2. Regulation of the Minister of Communication and Information (Permenkominfo).

   The Indonesian Ministry of Communication and Information also issues various regulations related to cyber security, including protection against malware. The Minister of Communication and Information Regulation regulates information and communication technology security standards that must be complied with by service providers and users of information technology in Indonesia.

3. National Cyber Security Policy.

   The Indonesian government has formulated a National Cyber Security Policy which sets out strategies and measures to protect the country's information infrastructure from cyberattacks, including malware attacks. This policy covers efforts to prevent, detect, and handle cyber security incidents as a whole.

4. National Cyber and Crypto Agency (BSSN).

   BSSN is the institution responsible for cyber security in Indonesia. BSSN has an important role in coordinating and implementing cyber security policies, including in handling malware attacks and related prevention efforts.

In existing regulations, law enforcement efforts against perpetrators of malware distribution are the main focus. The regulation also emphasizes the importance of cooperation between the government, related institutions, the private sector, and society in fighting the threat of malware. Apart from that, advancing public awareness about cyber security is also a priority in efforts to prevent malware attacks in Indonesia. With a comprehensive regulatory framework and collaborative efforts between various related parties, it is hoped that Indonesia can be more effective in protecting the public from malware threats and ensuring the security and sustainability of the use of information technology in this country.[8]

The problem in this paper is What is the Guarantee of Legal Protection for Malware Victims in Indonesia?

2 Method

2.1 Method

The method used in writing this applied paper is a descriptive-analytical method, namely by using data that clearly describes problems directly in the field, then analysis is conducted, and then conclusions are drawn to solve a problem. The data collection method is through observation and literature study to obtain solutions to problems in preparing this paper.

In line with the research objectives to be achieved, the domain of this research is included in the realm of qualitative research, thus a qualitative approach method will be used. According to Petrus Soerjowinoto et al., qualitative methods highlight the researcher's understanding process in problem formulation to construct a complex and holistic legal phenomenon.[9]

2.2 Approach

The sociological juridical approach, namely a juridical approach method used to examine problems from a legal and systematic perspective and as a guide to rules that can be used as a basis for analyzing legal phenomena that arise. The sociological approach is applied to study a problem in society or the community environment with the aim and objective of obtaining facts, which is followed by finding problems, identifying problems, and seeking solutions to problems. This research describes the situation of the object under study, namely focusing on Guaranteeing Legal Protection for Malware Victims in Indonesia in practice[10]. The approach methods used are the statutory approach and the case approach. Primary legal materials are obtained through statutory regulations, and secondary legal materials are obtained through books, scientific journals, and websites. Non-legal research materials were obtained from websites and social media. The research material that has been obtained is then analyzed descriptively.

3 Result and Discussion

3.1 Guarantee of Legal Protection for Malware Victims in Indonesia

Although law enforcement is guided by the law, it does not always lead to injustice because it can be manipulated. Law enforcement comes from society and aims to achieve peace and tranquility in society itself.[11] Law enforcement is an effort to make legal ideas and concepts that people hope for become a reality. Law enforcement is a procedure that involves many things.[12]

Increasing cyber security is not an absolute guarantee for society, government, and businesses to receive protection in utilizing cyberspace. Protection for cyberspace users must still be a priority. The government has formed laws and regulations to protect cyberspace users, however solving cyberspace issues is not an easy matter, because crimes in cyberspace are committed by communication.[13]. One way to provide a sense of security to internet users with technological developments is to know the appropriate legal protection procedures for internet users so that internet users can feel the benefits when surfing in cyberspace or making online

transactions in cyberspace[14]. Considering that current information has become a commodity, efforts to protect this asset are very necessary. One of the protection efforts is through criminal law, both with penal and non-penal means[15].

Protection and enforcement of cyber law on malware is regulated in Article 27 of the ITE Law which regulates actions that are prohibited from being carried out in cyberspace.

Article 27

(1) Every person intentionally and without right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents that contain content that violates morality.

(2) Every person intentionally and without authorization distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents that contain gambling content.

(3) Every person intentionally and without right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents that contain insulting and/or defamatory content.

(4) Every person intentionally and without right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents which contain extortion and/or threats.

Ransomware and Malware crimes are regulated in the provisions of Article 27 Paragraph (4) "Every person intentionally and without authority distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents which contain extortion and/or threats." Ransomware and Malware are categorized as criminal acts of extortion. Qualification of acts that are classified as extortion and threats in Article 368 paragraph (1) of the Criminal Code.

The direction and objectives of legal politics with the existence of Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) by the government is a political product that is created and packaged through rules that are formed and enforced in society as a whole and are binding on people who already have the terms and conditions to carry out their obligations to comply with these rules[1]. The principle states that politics and law must work together and strengthen each other with the motto, "Law without power is wishful thinking, power without law is despotism, it is mere utopia." This happens because in practice law often becomes a reflection (tool) for the will of political power holders. Even though in its application politics always "has its place" in terms of the formation of statutory regulations, politics, and the law should indeed coexist with each other in terms of the formation of statutory regulations, which many people view that the law is similar to power.[2]

Article 27 of Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) is an important legal basis for guaranteeing legal protection for the Indonesian people regarding electronic transactions, including protection from malware attacks. The following are several concrete steps that can be taken to realize the guarantee of legal protection by the Indonesian government following Article 27 of the ITE Law:

1. Effective Law Enforcement.

The Indonesian government needs to ensure effective law enforcement against perpetrators of spreading malware under the provisions of Article 27 of the ITE Law. This involves cooperation between law enforcement officials, related agencies, and the private sector to detect, prosecute, and prosecute perpetrators of computer crimes that harm society.

2. Public Education and Awareness.

   The government must educate the public about the risks of malware and the importance of cyber security. Through outreach and training campaigns, the public can be more aware of malware attacks and take appropriate preventive measures.

3. Security Technology Development.

   The government can encourage the development of security technology that can protect the public from malware attacks. Support for innovation in cyber security can help reduce vulnerability to malware attacks and increase the resilience of countries' information systems.

4. Collaboration with Related Parties.

   Collaboration between the government, related institutions, the private sector, and academics is very important in realizing legal protection guarantees by Article 27 of the ITE Law. Cross-sector collaboration can strengthen efforts to prevent and deal with malware attacks holistically.

5. Regulatory Monitoring and Evaluation.

   The government needs to regularly monitor and evaluate the effectiveness of regulations regarding legal protection from malware attacks. By carrying out ongoing evaluations, the government can adjust policies and law enforcement measures following developments in information technology and cyber security.

By executing these steps comprehensively and consistently, the Indonesian government can guarantee legal protection for people who are victims of malware by the provisions of Article 27 of the ITE Law. This is expected to improve cyber security, protect people's rights, and ensure the continued use of information technology in Indonesia.

Several possible obstacles that arise in realizing legal protection guarantees by the Indonesian government under Article 27 of the ITE Law are as follows:

1. Limited Resources.

   One of the main obstacles is limited resources, both in terms of budget, personnel, and infrastructure. Law enforcement against perpetrators of malware distribution requires significant costs and a trained workforce.

2. Technological Complexity.

   Malware attacks continue to develop with increasingly sophisticated techniques, so law enforcement officials need to keep abreast of these technological developments. Limited technical understanding and expertise in the field of cyber security can be an obstacle in dealing with malware attacks.

3. Cross-regional and international cooperation.

Malware attacks know no boundaries, so cross-regional and international cooperation is important. Coordination between countries in law enforcement against malware attacks can face obstacles such as regulatory, language, and cultural differences.

4. Personal Data Protection.

   In the law enforcement process against perpetrators of malware distribution, protecting the personal data of victims is also an important concern. Maintaining a balance between personal data protection and law enforcement efforts can be an obstacle in itself.

5. Understanding of the law is not yet optimal.

   Some parties may still not fully understand the legal implications of Article 27 of the ITE Law regarding malware attacks. Suboptimal understanding can hamper the law enforcement process and protection of malware victims.

6. Competing and Commercial Interests.

   Sometimes, competing and commercial interests between companies or entities can be an obstacle to law enforcement against malware attacks. This can slow down the process of investigating and taking action against perpetrators of computer crimes.

7. Legal and Ethical Challenges.

   There are also challenges in terms of legal and ethical enforcement in dealing with malware attacks, especially about privacy, freedom of expression, and human rights. The government needs to ensure that law enforcement efforts do not violate individual rights and applicable legal principles.

By identifying and overcoming these various obstacles proactively, the Indonesian government can be more effective in realizing guaranteed legal protection for people who are victims of malware by Article 27 of the ITE Law. Collaboration between various related parties and continuous efforts to increase law enforcement capacity in the field of cyber security are the keys to overcoming these obstacles.[8]

4 Conclusion

The importance of legal protection guarantees provided by the Indonesian government by Article 27 of Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE). Article 27 of the ITE Law is the legal basis that protects the Indonesian people in conducting electronic transactions, as well as regulating legal action against violations that occur in the digital realm. In realizing this guarantee of legal protection, the government needs to face various complex and diverse obstacles. These obstacles include limited resources, technological complexity, cross-regional and international cooperation, protection of personal data, suboptimal understanding of the law, commercial interests, as well as legal and ethical challenges. To overcome these obstacles, strategic steps are needed, such as increasing the effectiveness of law enforcement, educating the public about cyber security, developing security technology, cross-sector collaboration, and regular evaluation of regulations to adapt to technological developments.

Implementation of measures to guarantee protection from Malware can increase the effectiveness of guaranteed legal protection for the public related to electronic transactions and the use of information technology. In this way, it is hoped that the public can feel safer and protected when making online transactions, while the government continues to strive to maintain cyber security and protect individual rights by the spirit of the ITE Law. By paying attention to various existing obstacles and taking appropriate action, the Indonesian government can strengthen the legal protection system in the digital realm and ensure that people can enjoy the benefits of information technology safely and securely.

References

[1] Moh.Mahfud MD, *Politik Hukum Di Indonesia*. Jakarta: Rajawali Press, 2009.

[2] L. Bariroh., "Politik Hukum Nasional dan Hegemoni Globalisasi Ekonomi," *Jurnal Review Politik*, vol. 2, no. 2, 2012.

[3] H. Juwana, *Hukum Ekonomi dan Hukum Internasional*. Jakarta: Lentera Hati.

[4] K. B. Syariah and G. Ilmu, "No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title," no. september 2016, pp. 1–6.

[5] Q. D. Kusumawardani, "Perlindungan Hukum bagi Pengguna Internet terhadap Konten Web Umpan Klik di Media Online," *Jurnal Penelitian Hukum De Jure*, vol. 19, no. 1, p. 11, 2019, doi: 10.30641/dejure.2019.v19.11-30.

[6] Rizky Kertanegara., "Penggunaan Clickbait Headlone pada situs Berita dan Gaya Hidup Muslim Dream.co.id," *Komunikasi*, vol. 11, no. 1, 2018.

[7] Y. Edwin., "Lebih dari 50 persen pengguna internet masih tergoda clickbait," beritagar.id.

[8] N. Prakasa, "Policies to Overcome the Increase in Cyber Crime in The Era of Globalization Realize Public Security," in *Proceedings of the 3rd Multidisciplinary International Conference, MIC 2023, 28 October 2023, Jakarta, Indonesia*, EAI, 2023. doi: 10.4108/eai.28-10-2023.2341686.

[9] Dkk. Petrus Soerjowinoto, *Buku Panduan Metode Penulisan Karya Hukum (MPKH) dan Skripsi*. Semarang: Fakultas Hukum,UNIKA Soegijapranata, 2006.

[10] R. H. Soemitro, *Metodologi Penelitian Hukum dan Jurimetri*. Jakarta : Ghalia Indonesia, 1988.

[11] Robert B. Seidman & William J. Chambliss, *Law, Order and Power*. Massachusetts: Addison Wesley Publihing Compan, 1971.

[12] S. Dellyana, *Konsep Penegakan Hukum*. Yogyakarta: Liberty, 1988.

[13] Maskun, *Kejahatan CYber Crime Suatu Pengantar*. Jakarta: Kencana, 2013.

[14] Q. D. Kusumawardani, "Perlindungan Hukum Bagi Pengguna Internet Terhadap Konten Web Umpan Klik Di media Online," *Jurnal Penelitian Hukum DE JURE*, vol. 19, no. 1, 2019.

[15] Arief, *Tindak PIdana Mayantara: Perkembangan Kajian Cybercrime di Indonesia*. Jakarta: PT. Grafindo Persada., 2016.