TRANSPUBLIKA
Precise. Resilience. Felicitous.

Policy, Law, Notary and Regulatory Issues
https://ojs.transpublika.com/index.php/POLRI
Online ISSN 2809-896X

https://doi.org/10.55047/polri.v4i2.1633

Original Article

Juridical Review of Legal Protection for Victims of Mobile Malware Attacks through Digital Invitations

Arif Budianto[1*], Surya Nita[2]

[1,2]Police Science Study Program, School of Strategic and Global Studies, Universitas Indonesia, Jakarta, Indonesia
Email: [1)] arifbud.98@gmail.com

Received : 14 January - 2025
Accepted : 16 February - 2025
Published online : 19 February - 2025

Abstract

This research aims to analyze the characteristics of mobile malware attacks through digital invitations, evaluate legal regulations that protect victims in the Banten Police area, and identify obstacles and formulate solutions to improve the effectiveness of legal protection against cybercrime. With increasing cases of cybercrime in the region, this research combines a multidisciplinary approach through field research and normative legal research. Data were obtained from three main sources, namely interviews with victims, law enforcement officials, and legal experts (primary sources); official documents such as laws and regulations (secondary sources); and additional related literature (tertiary sources). Data collection techniques were conducted through observation, in-depth interviews, and documentation, which were then analyzed qualitatively through the stages of data reduction, data presentation, and conclusion drawing. The results showed that mobile malware attacks through digital invitations, which utilize phishing, smishing, and vishing techniques, have become a serious threat with a significant impact on financial security and user data privacy. Existing regulations, such as the Electronic Information and Transaction Law and the Personal Data Protection Law, still have limitations in providing effective protection, especially in the Banten Police area. The main obstacles identified include an imbalance in regulatory focus that focuses more on punishing perpetrators, a lack of technological infrastructure, and low public awareness of cyber threats. Therefore, this study recommends the need for regulatory revisions with an emphasis on victim protection, capacity building of law enforcement officers, public education on digital security, and international cooperation to deal with increasingly complex cybercrime.

Keywords: Mobile Malware, Digital Invitation, Legal Protection, Cybercrime.

1. Introduction

In today's digital era, individuals are faced with an abundance of information along with the rapid advancement of technology. The development of information technology, particularly in computer science and the internet, has created new networks that affect various aspects of life (Assiffa, 2023). Although Indonesia has experienced a surge in technology and information since 1994, the country still lags behind other industrialized countries. Older groups, often referred to as digital immigrants, have difficulty adapting to new technologies, making them vulnerable to various forms of cybercrime (Apidana et al., 2020).

The concept of telematics, which is the integration of telecommunications and informatics, has changed the way humans interact and communicate (Maskun et al., 2013). Although the internet brings great benefits, including easy access to information and increased efficiency in various fields, the threat of cybercrime is also increasing (Budiastanti, 2017). Cybercrime includes various illegal acts that utilize technology, such as data theft, online

fraud, and defamation (Andriani, 2023). In this context, cybercrime affects not only individuals, but also institutions and companies, posing serious challenges in the aspects of data protection and privacy.

According to a 2019 APJII survey, social media use is the main reason individuals access the internet, with 51.5% of respondents using the internet for this purpose (Lestari et al., 2022). However, along with the increase in internet usage, cybercrime cases have also increased, including the spread of increasingly sophisticated malware. One of the biggest threats currently developing is mobile malware attacks in the form of digital invitations through instant messaging applications such as WhatsApp. This attack exploits users' ignorance of technology by sending Android Package Kit (.apk) format files that allow the perpetrator to access the victim's personal data, including financial and banking information (BSSN, 2023).

In Indonesia, legal protection for victims of cybercrime is regulated in Law No. 19/2016 which amends Law No. 11/2008 on Electronic Information and Transactions. However, the effectiveness of the implementation of this law in handling cybercrime cases is still debatable. Various studies show that cybercrime continues to increase along with the development of digital technology, demanding the strengthening of regulations and stricter law enforcement (Septiani et al., 2016).

The development of digital technology in Indonesia has brought positive impacts in various aspects of life, but it is also accompanied by an increase in cybercrime threats, one of which is through malware attacks (Dalimunthe et al., 2022). Based on data from the fourth quarter of 2023, the most dominant type of malware in Indonesia is Trojan with 1,283 cases or about 32% of the total attacks. Trojans are known as malicious software that masquerades as legitimate programs to trick users and steal sensitive data. In addition, Generic type malware took second place with 754 cases (19%), followed by Adware (477 cases or 12%) which is often used to infiltrate malicious advertisements into victims' devices.

The existence of other malware such as Crack (10%), Infector (9%), as well as Worm and Vintage which each accounted for 6%, shows that threats to cybersecurity in Indonesia are increasingly diverse. In addition, Ransomware attacks that reached 147 cases (4%) are of particular concern because they are able to encrypt victim data and demand ransom for its recovery. The existence of Miner and Other categories with a smaller percentage also still indicates a threat that needs to be anticipated.

This phenomenon indicates that many users remain vulnerable to malware attacks, either due to a lack of awareness regarding the importance of digital security or weaknesses in the protection systems they use. Therefore, more effective mitigation strategies are needed, including regulatory measures, public awareness campaigns, and the strengthening of security technologies to counter these evolving threats.

Cybercrime cases in Indonesia have been increasing alongside the advancement of digital technology. One prevalent form of cybercrime involves fraud, data theft, and money laundering through fake courier MOD AP applications. According to Police Report Number LP/A/0747/XII/2022/SPKT.Dittipidsiber/Bareskrim Polri, dated December 20, 2022, the Cyber Crime Directorate (Dittipidsiber) of the Indonesian National Police's Criminal Investigation Agency (Bareskrim Polri) conducted an investigation into this crime method. Perpetrators spread malicious links or applications through social media, particularly WhatsApp, by impersonating courier services. When victims download and open these applications, the perpetrators can steal sensitive data, such as One-Time Passwords (OTP) from SMS messages, and gain unauthorized access to their bank accounts.

The investigation found that several applications were involved in this crime, including Cek Paket.apk, Cek Resi J&T.apk, and FOTO PAKET.apk. To combat this case, law enforcement conducted operations across multiple regions, including South Sulawesi, South Sumatra, Riau, Lampung, and East Java. A total of 13 suspects, identified by their initials—RR, WEY, AI, AK, AD, E, S, R, W, R, RK, NP, and H—were apprehended between December 31, 2022, and January 13, 2023. This case serves as evidence that cybercrime continues to evolve with increasingly sophisticated methods, emphasizing the need for stronger legal measures to protect the public from similar threats in the future.

Various previous studies have examined the phenomenon of cybercrime from various perspectives, ranging from the implementation of the Electronic Information and Transaction Law (UU ITE) in overcoming mobile malware-based fraud (Sastrawan, 2024) to efforts to socialize and increase public understanding of the characteristics of cybercriminals (Habib et al., 2024). Research by Sastrawan (2024) revealed that the implementation of the ITE Law on fraud cases through the WhatsApp application in Buleleng Regency is still not running efficiently, mainly due to limited technological resources and lack of coordination between institutions. On the other hand, studies on legal protection in the banking sector, such as those conducted by Assiffa (2023) and Kurniawan & Soeskandhi (2022), show the vulnerability of the banking system to cybercrime attacks, resulting in service disruptions and losses to customers. In addition, research that examines the technical aspects of wiretapping on the WhatsApp application (Safrizal et al., 2022) and challenges of law enforcement in social media abuse (Muhammad et al., 2022) highlighted the importance of increasing the capacity of law enforcement officials and the need for a more comprehensive preventive approach. These previous normative and descriptive studies, including juridical studies by Budiastanti (2017) and Pambudi & Iksan (2020), have provided an overview of the weaknesses of existing regulations in anticipating cybercrime. However, although there have been many analyses of legal and technical aspects, there is a void of research that integrates empirical approaches with multidimensional analysis of technical, juridical, and socio-cultural aspects to identify strategic solutions for the enforcement of the ITE Law and more effective legal protection in the digital era. This gap is the background and motivation for the research to be carried out, in order to provide a more holistic contribution to tackling cybercrime in Indonesia (Abidin, 2015; Andriani, 2023).

This research aims to analyze the characteristics of mobile malware attacks through digital invitations, evaluate legal regulations that protect victims in the Banten Police area, and identify obstacles and formulate solutions to improve the effectiveness of legal protection against this cybercrime. The selection of this region is based on the increasing number of cybercrime cases in the area, which indicates the need for more effective policies in dealing with digital attacks. With a multidisciplinary approach that combines aspects of law, information technology and cybersecurity, this research seeks to contribute to improving protection for victims of cybercrime in Indonesia.

2. Methods

2.1. Research Type

This research combines two main approaches, namely field research and normative legal research (Ibrahim, 2006). The field research method is used to collect data directly through on-site observations and interviews, which allow researchers to see and record real phenomena that occur in the context of legal protection of cybercrime victims. Meanwhile, normative legal research relies on the analysis of written legal sources, such as laws,

regulations, and legal literature, to test the consistency and suitability of existing legal norms. By combining these two approaches, the research is able to provide a comprehensive picture from both the empirical and theoretical sides.

2.2. Data Source

The data sources in this study are categorized into three types:

a) Primary Legal Sources: Data obtained directly through interviews with key stakeholders, such as cybercrime victims, law enforcement officers, and legal experts. This interview technique allows researchers to gather authentic information and firsthand experiences regarding case handling.

b) Secondary Legal Sources: Official documents, including laws, regulations, and policies, such as the 1945 Constitution, the Indonesian Criminal Code (KUHP), Law No. 2/2002 on the Indonesian National Police (POLRI), Law No. 19/2016, Law No. 11/2008 on Electronic Information and Transactions, and Law No. 27/2022 on Personal Data Protection. This secondary data is analyzed to understand the existing legal framework and its relevance to victim protection.

c) Tertiary Legal Sources: Supplementary literature, including books, journals, articles, and case studies related to legal protection in the context of cybercrime. These tertiary sources help researchers expand their perspectives and obtain comprehensive supporting information.

2.3. Data Collection Technique

Various data collection techniques were employed to obtain in-depth and valid information, including:

a) Observation: This technique involves directly observing interactions and case-handling processes in the field, such as visits to police stations or cybercrime complaint centers. Observations provide insights into real conditions and dynamics, including nonverbal behaviors and the surrounding context of mobile malware cases.

b) Interviews: In-depth interviews were conducted with various relevant parties, including victims, law enforcement officers, and legal experts. This technique allows researchers to collect qualitative data in the form of experiences, perceptions, and viewpoints regarding the investigation process, judicial proceedings, and legal protection efforts in cybercrime cases.

c) Documentation: Data collection was also carried out through the study of official documents, case reports, court rulings, and academic publications. This documentation technique helps researchers gather verifiable written data to support their analysis.

2.4. Data Analysis Technique

After data collection, the researcher applied qualitative data analysis techniques involving three main stages:

a) Data Reduction: In this stage, the collected data is selected, summarized, and focused on information most relevant to the research questions. This process involves identifying themes and patterns emerging from observations, interviews, and documentation.

b) Data Presentation: The reduced data is then systematically presented in the form of narratives, tables, or diagrams. This presentation aims to facilitate understanding and provide a clear overview of the findings obtained from field research and legal documents.

c) Conclusion Drawing: The final stage of analysis involves drawing conclusions based on the integration of the presented data. The researcher verifies and confirms the findings to answer the research questions and formulate relevant policy recommendations to enhance legal protection for cybercrime victims.

3. Results and Discussion

3.1. Characterizing mobile malware attacks through digital invitations as a form of cybercrime

Mobile malware attacks pose a serious threat to Indonesians as smartphones are increasingly used in various aspects of life, including financial transactions and personal communications (Fazlurrohman et al., 2024). Common types of malware include phishing, smishing, and vishing, which use manipulative techniques through emails, text messages, and phone calls to deceive users into revealing sensitive information (Hakim & Setiawan, 2024). Unfortunately, low awareness of cybersecurity exacerbates the situation, leaving many users vulnerable to these attacks (Wiryawan et al., 2019). The impact of a mobile malware attack is significant, especially in terms of financial and data privacy. From an economic perspective, these attacks can cause huge financial losses to individuals and organizations due to data breaches and fraudulent activities (Zakaria & Zolkipli, 2021). In addition, the risk of leakage of personal information stored on mobile devices is also higher, sparking concerns about privacy breaches and data misuse (Agarwal et al., 2022). As such, effective mitigation measures, such as increasing user awareness and implementing stricter security policies, are needed to protect the public from the threat of mobile malware.

Mobile malware attacks through digital invitations, such as SMS phishing (smishing) and social networking messages, have become an increasingly complex form of cybercrime. These attacks exploit the social nature and high connectivity of mobile devices by distributing malicious links or software that can steal data and remotely control devices. One of the main propagation methods is through social networks, where mobile botnets such as SocellBot use online messaging systems to recruit and control bots, making detection by security systems difficult (Faghani & Nguyen, 2019). In addition, smishing methods are often used by perpetrators by sending text messages containing malicious links or fake contact information to trick users into providing their sensitive data (Mishra & Soni, 2019). Android-based devices are prime targets for SMS-based malware, which allows attackers to steal and manipulate victim data through malicious apps or links sent via SMS (Kumar et al., 2023).

In terms of the type of malware used, mobile-based botnets pose a serious threat as they are capable of spreading through various communication channels, including SMS, Bluetooth and WiFi. This type of malware allows attackers to remotely control victims' devices and collect their personal information (Tidke et al., 2017). In addition, some malware is hidden in repackaged applications, i.e. legitimate applications that have been modified to include malicious code, often leading to user privilege escalation and financial loss (Penning et al., 2014).

The main characteristic of these attacks is the use of social engineering as a manipulative technique to gain the trust of the victim. Perpetrators often utilize social media platforms and messaging apps to send fake invitations containing malicious links or APK files designed to trick users into downloading malware (Burton & Moore, 2024; Guaña-Moya et al., 2022). Once the malware is installed, it can gain access to sensitive information such as passwords and banking data, as well as allow remote control of the victim's device (Al-Sinayyid et al.,

2023). Some types of malware even have the ability to hide within the system, remaining active even after restarting the device (Ajayi et al., 2023).

The impact of mobile malware attacks through digital invitations is significant for victims. They can experience personal data theft, financial fraud, and even be subjected to ransomware attacks, where their data is encrypted and the perpetrator demands a ransom for its recovery (Chen et al., 2015). In addition, the anonymity of perpetrators poses a major challenge to law enforcement, as they often use VPNs and offshore servers, making it difficult for authorities to track and prosecute perpetrators (Burton & Moore, 2024). With the increasing sophistication of this attack method, stronger legal regulations are needed as well as efforts to increase public awareness in avoiding the threat of mobile malware.

3.2. Legal regulations governing the protection of victims of mobile malware attacks in the Banten Police Region

The legal framework for tackling cybercrime in Indonesia is based on several key regulations, such as the Electronic Information and Transactions Law (ITE) and the Personal Data Protection Law. The ITE Law focuses on preventing and prosecuting perpetrators of digital crimes, but is often criticized for not providing enough protection for victims, especially regarding restitution and compensation (Apriandi et al., 2024; Wahyudi, 2013). Meanwhile, the Personal Data Protection Law, which was passed in 2022, offers a more comprehensive protection mechanism, particularly in the case of cybercrime such as fraud through mobile malware (Hakim & Setiawan, 2024).

Digital app-based scams are on the rise, with one of the most prevalent modes being digital wedding invitations with malware inserted. The latest case happened to a vehicle accessory businessman from Malang who suffered financial losses due to a digital invitation containing malware distributed via WhatsApp. In this context, legal protection for victims of mobile malware-based fraud is very important because mobile devices store various sensitive information used for financial transactions (Minarosa, 2022). Technological advancements demand an adaptive legal framework to protect mobile software and operating systems from malware threats (Jing et al., 2019). Behavior-based analysis methods for mobile malware are crucial in detecting and blocking new malware, thereby improving users' security and the privacy of their data (Graham, 1984; Sui & Guo, 2012). More specific regulations against digital invitation-based malware need to be developed to prevent the exploitation of technology in fraud cases.

In the Indonesian legal system, mobile malware-based fraud can be charged with various statutory provisions. Analysis of the legal regulations for the protection of victims of mobile malware attacks in the Banten Police area shows the complexity of the interaction between various existing legal instruments and the dynamics of cybercrime that continue to develop. Fundamentally, the Electronic Information and Transaction Law (ITE) and the Personal Data Protection Law are the main legal umbrellas governing electronic transactions and data protection. In the context of malware-based fraud, Article 378 of the Criminal Code serves as the basis for taking action against perpetrators through criminal mechanisms, while Article 263 of the Criminal Code can be applied to cases of spreading false information that harms victims. Thus, the victim has the option to report the incident to law enforcement officials in order to obtain justice and appropriate sanctions against the perpetrator (Susanto et al., 2022).

In addition to criminal regulations, legal protection for victims is also regulated through consumer protection mechanisms. Consumer Protection Law No. 8/1999 gives consumers the right to obtain accurate information and compensation for losses suffered. This is further strengthened by the application of Article 28 paragraph (1) of the ITE Law, which threatens

criminal sanctions of up to six years in prison and a maximum fine of Rp1 billion for those who intentionally spread false information. The role of consumer law is very important considering that digital crimes often target individual interests in electronic transactions, so protection in this area must be integrated with criminal law enforcement efforts.

Banking sector regulations also play a strategic role in dealing with cybercrime, especially through Bank Indonesia Regulation Number 22/20/PBI/2020 concerning Consumer Protection in the Financial Services Sector. This regulation guarantees customers' rights to obtain transparent information and professional services, and provides a mechanism for filing claims for unauthorized digital transactions. Thus, victims of malware-based fraud can not only rely on criminal channels, but can also claim compensation through civil proceedings, which is part of a comprehensive dispute resolution effort.

However, there are still normative ambiguities in the legal protection of cybercrime victims. One of the main challenges is the lack of clarity in categorizing victims as consumers, especially when there is an agreement or terms of service established between the victim and the bank. This ambiguity often limits the compensation claims that victims can file. In addition, the legal lacuna in defining digital fraud specifically leads to difficulties in proof and enforcement, allowing cybercriminals to exploit this loophole to avoid legal liability.

The Criminal Code has regulated the crime of fraud in Article 378, which generally defines fraud as an attempt to obtain unlawful gain by using false identity or deception. However, the application of this article to online fraud cases, such as fake job vacancy scams or fictitious online businesses, shows a legal gap because this regulation has not specifically regulated the modus operandi of cybercrime. The revision of the ITE Law through Law No. 19/2016 is an attempt by the government to provide stronger protection against cybercrime. However, the revision was criticized for not providing an explicit definition of online fraud, making law enforcement less effective in practice (Susanto et al., 2022).

The absence of the term "*fraud*" explicitly in several articles of the ITE Law creates loopholes that are utilized by digital criminals. Although Article 28 paragraph (1) provides a legal basis to take action against the disseminators of false information, this lack of definition indicates the need for further revision so that legal protection can cover all forms of digital crime. To this end, collaboration between the government, legal institutions and the public is essential in building a better understanding of cyber threats and creating a safe and trusted digital environment. This synergy should also involve the technology industry, which has a vital role in tracking and countering malware attacks.

In addition to challenges in the normative aspect, the implementation of the ITE Law in dealing with mobile malware-based fraud faces various practical obstacles. These include difficulties in tracing the source of the malware, collecting sufficient digital evidence, and the complexity of legal procedures in processing cybercrime cases. These obstacles require an increase in the capacity of law enforcement officials as well as the development of supporting technology that is able to respond to the dynamics of cyber attacks in real time. Thus, regulatory updates must be accompanied by increased competence and cross-sectoral cooperation, to ensure that every cybercriminal can be prosecuted effectively and victims can recover for their losses.

Overall, the legal protection of victims of mobile malware attacks in the Banten Police area is a challenge that requires a multi-disciplinary approach. Existing regulations-ranging from the Criminal Code, ITE Law, Consumer Protection Law, to banking regulations-must continue to be refined in order to accommodate the development of digital technology and cybercrime modus operandi. More explicit regulatory updates and synergy between the

government sector, law enforcement officials, and the technology industry are key in creating a safe digital environment and providing justice for all victims of cybercrime.

Legal regulations governing the protection of victims of mobile malware attacks in the Banten Police Region can be analyzed through the perspective of law enforcement theory, legal protection, and criminology. Based on the theory of law enforcement as social engineering (Soekanto, 1983), the law is expected to be an instrument of social change that shapes people's behavior to be more aware of cyber threats. However, in the context of applicable regulations in Indonesia, especially the Electronic Information and Transactions Law (ITE Law) and the Personal Data Protection Law (PDP Law), the emphasis is still more on imposing sanctions on perpetrators rather than encouraging prevention through education and public awareness. This shows that the law has not fully functioned as an effective social engineering tool in shaping safer digital behavior.

From the perspective of legal protection theory (Hadjon, 1987), regulations in Indonesia, including in the Banten Police Region, prioritize a repressive approach in dealing with cybercrime, while preventive protection for victims is still less than optimal. For example, although the ITE Law regulates sanctions against the dissemination of false information and illegal access to electronic systems, restitution and compensation mechanisms for victims of mobile malware attacks remain unclear. The Consumer Protection Law also provides victims with the right to protection, but the implementation and mechanism for claiming losses due to cyberattacks remains ineffective. This shows that regulations need to be more directed towards preventive protection aspects, such as strengthening digital security policies and providing compensation for victims of cyber crime.

From the point of view of criminology theory, especially Durkheim and Merton's anomy theory, existing regulations have not been able to fully accommodate social changes due to the rapid development of digital technology. Mobile malware attacks develop in the context of deregulation or an imbalance between technological developments and existing legal policies, thus creating a gap for cyber criminals to exploit victims. In addition, based on Sutherland's differential association theory, the modus operandi of malware attacks through digital invitations shows that cybercrime spreads through social networks and digital communication, but existing regulations are not sufficient to effectively control this pattern of crime spread.

In the context of social control theory (Hirschi & Stark, 1969), regulations in Indonesia, including in the Banten Police Region, still face challenges in establishing an effective control mechanism against cybercrime. Low public awareness and weak regulations on the supervision of digital platforms are the main factors that make this crime continue to grow. For example, although Bank Indonesia has implemented consumer protection regulations in digital transactions, many victims of malware attacks continue to suffer financial losses without a clear recovery mechanism. This suggests that regulations need to be further strengthened with stricter social control strategies, both through more adaptive cybersecurity policies and increased public digital literacy.

Overall, legal regulations governing the protection of victims of mobile malware attacks in the Banten Police Region still have various limitations when linked to legal and criminological theories. The law has not been fully effective in preventing cybercrime because it focuses more on repressive aspects than preventive. In addition, regulations are still less adaptive in the face of rapid technological change, which causes a high level of community vulnerability to mobile malware attacks. Therefore, policy revisions are needed that place more emphasis on victim protection, increased social control, and harmonization of

regulations with the development of digital technology so that legal protection for victims of cybercrime can be more optimal.

3.3. Challenges in the Implementation of Legal Protection for Victims of Mobile Malware Attacks in the Jurisdiction of Banten Regional Police

The rapid development of digital technology has increased the risk of cyberattacks, including mobile malware attacks that target users' mobile devices. In the jurisdiction of Banten Police, the implementation of legal protection for victims of these attacks still faces various obstacles covering aspects of regulation, law enforcement, and public awareness. These obstacles not only slow down the response to cybercrime but also hinder the restoration of the rights of victims who have suffered losses due to these attacks.

In the context of legal protection theory (Hadjon, 1987), the main obstacle lies in the imbalance between preventive and repressive protection. Existing regulations focus more on the criminal aspect in taking action against cyber criminals, but have not provided a clear compensation mechanism for victims. As a result, many victims of mobile malware attacks in the Banten Police Region experience difficulties in recovering the losses suffered, both in terms of financial and data protection rights. This reflects that the applicable legal system is still reactive and has not fully accommodated the need for legal protection for victims of digital crime.

One of the main problems in legal protection for victims of mobile malware attacks is the imbalance of regulatory focus that prioritizes the aspect of punishing the perpetrator compared to the protection of victims. Indonesia's Electronic Information and Transaction Law (UU ITE), for example, mostly regulates sanctions for cybercriminals but has not explicitly regulated compensation or restitution mechanisms for victims of mobile malware attacks. This creates a gap in the legal system, where victims are often left without adequate legal support after suffering financial or data losses due to malware attacks.

Apart from the regulatory aspect, challenges also arise in the realm of law enforcement. One of the main obstacles is the limited human resources and technological infrastructure in dealing with cybercrime effectively. Law enforcement officers in Banten Police still face limitations in terms of specialized training related to detection, investigation, and data recovery of victims of malware attacks. Without adequate technical skills, investigations into cases of mobile malware attacks often encounter obstacles, both in identifying perpetrators and in proving crimes in the digital realm. In addition, suboptimal technological infrastructure further exacerbates the situation, especially in terms of monitoring data traffic and coordination with related institutions in cyber law enforcement.

Based on the theory of law enforcement as social engineering (Soekanto, 1983), one of the main challenges in law enforcement against cybercrime is the lack of effectiveness of regulations in shaping public awareness and behavior related to digital security. The applicable regulations are still oriented towards the aspect of punishing perpetrators, while preventive strategies, such as cyber education and digital literacy, have not been implemented optimally. This shows that the law has not fully functioned as an instrument of social change that can significantly reduce the rate of cybercrime.

From the perspective of Hirschi & Stark (1969) social control theory, the obstacles in implementing legal protection for cybercrime victims are also related to the weak external and internal control systems in overseeing people's behavior in the digital ecosystem. Low public awareness of the risks of cybercrime and the lack of regulations governing digital security standards have led to an increase in the frequency of mobile malware attacks. If stricter social control mechanisms, such as policies governing application security and digital transactions, can be implemented more systematically, the risk of cybercrime can be minimized more

effectively. Low public awareness of the threat of cybercrime is also an inhibiting factor in the implementation of legal protection for victims. Many victims of mobile malware attacks do not realize that they have legal rights to obtain protection and compensation for their losses. This lack of understanding contributes to the lack of reporting cases to the authorities, making it difficult to accurately map the scale of mobile malware threats in the Banten Police area. Without sufficient data on attack incidents, it is difficult to develop effective legal protection policies.

Furthermore, existing legal provisions are not fully relevant in specifically addressing mobile malware attacks. The ITE Law and related regulations mostly regulate cybercrime in general, without providing specific definitions and treatments for mobile malware attacks. As a result, law enforcement officials often face difficulties in ensnaring perpetrators using existing articles, especially if the attacks are carried out across national borders. Cybercrimes involving actors from multiple jurisdictions require uniform legal standards to be effectively prosecuted. However, to date, there is no international mechanism that comprehensively regulates mobile malware attacks, so cooperation between countries in tackling this crime is still limited.

To overcome these obstacles, several steps need to be taken to improve the effectiveness of legal protection for victims of mobile malware attacks in the Banten Police area. First, a revision of existing regulations is needed to further emphasize aspects of victim protection, including the provision of compensation and recovery mechanisms for those affected (Irawan et al., 2019). Second, increasing the capacity of human resources in the field of cybercrime is needed, both through technical training for law enforcement officials and strengthening technological infrastructure to support the investigation and prosecution of mobile malware criminals (Supriyadi et al., 2022).

Third, it is important to raise public awareness of the threat of mobile malware and their rights to legal protection. Educational campaigns on digital security and incident reporting procedures can help people be more aware of the risks of cybercrime and be more proactive in reporting attacks they experience (Kurniawan & Setiyono, 2023). In addition, an adaptive approach in policy updates is also needed so that regulations can continue to adapt to dynamic technological developments. Flexible regulations that are able to accommodate new threats will help improve the effectiveness of legal protection for victims (Troshchenkov & Halona, 2024).

Cross-border cooperation is also one of the main strategies in dealing with mobile malware crime, given its often international scale. Harmonizing policies between countries can strengthen law enforcement mechanisms against cybercriminals, especially in taking action against actors operating outside of Indonesia's jurisdiction (Troshchenkov & Halona, 2024). In addition, the accountability of technology companies must also be improved, especially in terms of protecting user data and increasing system security to prevent exploitation through mobile malware.

With the implementation of these strategies, it is hoped that legal protection for victims of mobile malware attacks can be optimized and responsive to evolving challenges. However, it is important to remember that cybercrime is a dynamic and evolving phenomenon. Therefore, protection efforts must be carried out in a sustainable manner with a combination of a strong legal approach, increased law enforcement capacity, and broad public education. Thus, victims of mobile malware attacks, especially in the Banten Police area, can obtain more effective and equitable legal protection in the future.

If associated with Durkheim and Merton's anomy theory, the obstacles in the implementation of legal protection for victims of cybercrime can be explained through the

imbalance between the development of digital technology and the ability of regulations to adapt to these changes. Mobile malware attacks continue to evolve with increasingly complex methods, while existing legal tools have not been able to fully accommodate the dynamics of the perpetrators' modus operandi. This mismatch creates an anomy condition, where prevailing norms and regulations are no longer effective enough to control behavior in the digital ecosystem. The absence of adaptive regulations also opens up legal loopholes that can be utilized by perpetrators to avoid legal liability.

Furthermore, Sutherland's differential association theory can explain how cybercrime, including malware attacks through digital invitations, evolve through social networks and technology-based communication. These attacks exploit victims' social trust in messages or links sent by individuals they know, increasing the likelihood of victims being tricked. However, law enforcement officials in the Banten Police Region face challenges in identifying and arresting perpetrators due to the anonymous nature of cybercrime and cross-border networks. In addition, limitations in the capacity of digital forensic technology hamper the process of investigating and proving crimes, thus reducing the effectiveness of law enforcement against these cases.

Overall, challenges in the implementation of legal protection for victims of mobile malware attacks in the Banten Police Region are not only rooted in the limitations of regulations, but are also influenced by low public awareness, limited capacity of law enforcers, and the lag of regulations in adjusting to the dynamics of digital technology development. Therefore, a more comprehensive and integrative approach is needed by combining legal, social and technological aspects to ensure more effective and responsive legal protection against the increasingly complex threat of cybercrime.

4. Conclusion

Based on the research findings, mobile malware attacks through digital invitations have become a serious threat to mobile device users in Indonesia. Attack techniques such as phishing, smishing, and vishing are becoming increasingly sophisticated, leveraging social engineering to deceive victims into providing sensitive information. The impact of these attacks is significant, particularly in terms of financial losses and data privacy, where victims may suffer from personal information theft and economic losses due to fraudulent activities.

Existing legal regulations, such as the Electronic Information and Transactions (ITE) Law and the Personal Data Protection Law, still have limitations in providing effective protection for victims. In the jurisdiction of the Banten Regional Police, the main challenges in implementing legal protection include regulatory imbalances that focus more on punishing perpetrators rather than protecting victims, a lack of technological infrastructure, and low public awareness of cyber threats. Additionally, these crimes are often committed across national borders, making law enforcement efforts more challenging.

Therefore, regulatory revisions that emphasize victim protection, enhanced capacity for law enforcement officers, public education on digital security, and international cooperation in combating mobile malware-based cybercrime are necessary. Through a holistic and collaborative approach, it is expected that the protection of mobile malware attack victims can be more effective and responsive to the ever-evolving technological challenges.

5. References

Abidin, D. Z. (2015). Kejahatan dalam Teknologi Informasi dan Komunikasi. *Jurnal Processor*, *10*(2), 509–516.

Agarwal, P., Nair, A., Jaiswal, S., Batra, N., & Grover, P. (2022). *Malware analysis in mobile devices*. https://doi.org/10.1049/icp.2022.0604

Ajayi, A., Olajide, M., Afolabi, O. P., & Abiodun, O. A. (2023). Evaluation of Phishing Attack Strategies on Mobile Device Users. *International Journal of Computer and Information Technology (2279-0764)*, *12*(1). https://doi.org/10.37502/ijsmr.2024.7911

Al-Sinayyid, A., Jewel, M. J. A., Mannuru, V., & Sasidhar, K. (2023). Defending Characteristics and Attribution Analysis for Phishing Attacks. *2023 International Conference on Computational Science and Computational Intelligence (CSCI)*, 868–874. https://doi.org/10.1109/csci62032.2023.00145

Andriani, N. (2023). Cybercrime Kejahatan Yang Berbasis Komputer. *Jurnal Hukum Non Diskriminatif*, *1*(2), 39–43.

Apidana, Y. H., Suroso, A., & Setyanto, R. P. (2020). Model penerimaan teknologi mobile payment pada digital native dan digital immigrant di Indonesia. *Jurnal Ekonomi, Bisnis, Dan Akuntansi*, *21*(4).

Apriandi, M., Sagala, R. V., & Basuki, B. (2024). Perlindungan Hukum Bagi Korban Cybercrime Penyebaran Data Pribadi Secara Online. *SINERGI: Jurnal Riset Ilmiah*, *1*(11), 1069–1079.

Assiffa, B. A. (2023). *Perlindungan Hukum Terhadap Nasabah Bank Syariah Indonesia Dari Serangan Cybercrime*. Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta.

Budiastanti, D. E. (2017). Perlindungan Hukum Terhadap Korban Tindak Pidana Penipuan Melalui Internet. *Jurnal Cakrawala Hukum*, *8*(1), 22–32.

Burton, S. L., & Moore, P. D. (2024). Pig butchering in cybersecurity: A modern social engineering threat. *SocioEconomic Challenges*, *8*(3), 46. https://doi.org/10.61093/sec.8(3).46-60.2024

Chen, G., Zhou, G., Mao, Z., Liu, Q., Zheng, Z., Chen, G., & Qin, P. (2015). Research of Social Engineering Attacks in Telecommunications Fraud. *2015 International Conference on Social Science, Education Management and Sports Education*, 1869–1872. https://doi.org/10.2991/SSEMSE-15.2015.477

Dalimunthe, S. R., Pujawati, S. A., & Sitorus, A. S. A. (2022). Technical Security in ITE Law and Copyrights of Devices and Systems. *POLICY, LAW, NOTARY AND REGULATORY ISSUES (POLRI)*, *1*(2). https://doi.org/10.55047/polri.v1i2.124

Faghani, M. R., & Nguyen, U. T. (2019). Mobile botnets meet social networks: design and analysis of a new type of botnet. *International Journal of Information Security*, *18*, 423–449. https://doi.org/10.1007/S10207-018-0412-6

Fazlurrohman, M. A., Nita, S., & Aminanto, M. E. (2024). Comparative Studies on Trends and Strategies for Combating Cybercrime Between Indonesia and Developed Countries. *POLICY, LAW, NOTARY AND REGULATORY ISSUES*, *3*(4), 498–515. https://doi.org/10.55047/polri.v3i4.1512

Graham, R. L. (1984). The legal protection of computer software. *Communications of the ACM*, *27*(5), 422–426.

Guaña-Moya, J., Chiluisa-Chiluisa, M. A., del Carmen Jaramillo-Flores, P., Naranjo-Villota, D., Mora-Zambrano, E. R., & Larrea-Torres, L. G. (2022). Ataques de phishing y cómo prevenirlos Phishing attacks and how to prevent them. *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6. https://doi.org/10.23919/cisti54924.2022.9820161

Habib, H. N., Efendi, A., & Prasetyo, D. E. (2024). Sosialisasi Fenomena Kejahatan Cyber dan Langkah Penanggulangan Sebagai Bentuk Antisipasi. *APPA: Jurnal Pengabdian Kepada Masyarakat*, *1*(5), 393–399.

Hadjon, P. M. (1987). *Perlindungan hukum bagi masyarakat Indonesia*. PT Bina Ilmu.

Hakim, A. A., & Setiawan, D. A. (2024). Perlindungan Korban Kejahatan Penipuan Online Bermodus Apk (Android Package Kit) melalui Whatsapp. *Jurnal Riset Ilmu Hukum*, *4*(1), 23–28. https://doi.org/10.29313/jrih.v4i1.3778

Hirschi, T., & Stark, R. (1969). Hellfire and delinquency. *Social Problems*, *17*(2), 202–213.

Ibrahim, J. (2006). Teori dan metodologi penelitian hukum normatif. *Malang: Bayumedia Publishing*, *57*.

Irawan, H., Wahyuningsih, S. E., & Hafidz, J. (2019). Legal Protection For Victims Of Traffic Violations That Lead To Death (Case Study On Police Traffic of Rembang). *Jurnal Daulat Hukum*, *2*(4), 485–492. https://doi.org/10.30659/JDH.2.4.485

Jing, R., Chen, J., & Liu, Y. (2019). *Proactive protection of mobile operating system malware via blocking of infection vector*. Google Patents.

Kumar, A., Sharma, I., & Sharma, A. (2023). Understanding the behaviour of android sms malware attacks with real smartphones dataset. *2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA)*, 655–660. https://doi.org/10.1109/ICIDCA56705.2023.10099595

Kurniawan, A. B., & Soeskandhi, H. (2022). Perlindungan Hukum Kepada Pengguna Elektronik Banking Atas Kejahatan Carding Ditinjau Dari Undang-Undang Informasi dan Transaksi Elektronik. *SUPREMASI: Jurnal Hukum*, *5*(1), 64–87.

Kurniawan, D., & Setiyono, J. (2023). Implementation of Human Rights Protection against Victims of Severe Human Rights Violations in Indonesia's Criminal Justice System. *International Journal of Social Science And Human Research*, *6*(7), 4033–4038. https://doi.org/10.47191/ijsshr/v6-i7-20

Lestari, U., Hamzah, A., & Sholeh, M. (2022). Sosialisasi Fenomena Cyber Crime dan Penanggulangannya Bagi Pengelola Informasi Publik Kapanewon Mlati Sleman Yogyakarta. *NEAR: Jurnal Pengabdian Kepada Masyarakat*, *1*(2), 100–106.

Maskun, M., Manuputty, A., Noor, S. M., & Sumardi, J. (2013). Kedudukan Hukum Cyber Crime Dalam Perkembangan Hukum Internasional Kontemporer. *Masalah-Masalah Hukum*, *42*(4), 511–519.

Minarosa, M. (2022). Legal Protection of Personal Data Owners as Cybercrime Victims Based on regulations regarding Electronic Information and Transactions. *Proceedings of the First Multidiscipline International Conference, MIC 2021, October 30 2021, Jakarta, Indonesia*.

Mishra, S., & Soni, D. (2019). SMS phishing and mitigation approaches. *2019 Twelfth International Conference on Contemporary Computing (Ic3)*, 1–5. https://doi.org/10.1109/IC3.2019.8844920

Muhammad, R. N., Mutalib, A., & Abdullah, R. H. (2022). Cyber Security Challenges in Law Perspective "Challenges of Criminal Law Enforcement in Misuse of Social Media (Medsos)." *Megafury Apriandhini, SH, MH Chair of 4th OSC*, 52.

Pambudi, R., & Iksan, M. (2020). *Tinjauan Yuridis Perlindungan Hukum Bagi Korban Cyber Crime*. Universitas Muhammadiyah Surakarta.

Penning, N., Hoffman, M., Nikolai, J., & Wang, Y. (2014). Mobile malware security challeges and cloud-based detection. *2014 International Conference on Collaboration Technologies and Systems (CTS)*, 181–188. https://doi.org/10.1109/CTS.2014.6867562

Safrizal, D. G., Aisyah, N., Putra, A. S., Valentino, V. H., & Prasetyo, B. S. (2022). Analisis Penyadapan pada Aplikasi WhatsApp Menggunakan Sinkronisasi Data. *Jurnal Esensi Infokom Vol*, *6*(1).

Sastrawan, W. D. (2024). *Implementasi Undang-Undang ITE No 19 Tahun 2016 Terkait Penipuan Menggunakan Mobile Malware Pada Aplikasi Whatsapp Di Kabupaten Buleleng*. Universitas Pendidikan Ganesha.

Septiani, D., Widiyasono, N., & Mubarok, H. (2016). Investigasi Serangan Malware Njrat Pada

PC. *J. Edukasi Dan Penelit. Inform. JEPIN*, *2*.

Soekanto, S. (1983). *Pribadi dan Masyarakat*. Alumni.

Sui, A.-F., & Guo, T. (2012). A behavior analysis based mobile malware defense system. *2012 6th International Conference on Signal Processing and Communication Systems*, 1–6.

Supriyadi, A., Alamsah, N., Nurasa, H., & Pancasilawan, R. (2022). Implementation of Law Enforcement and Disciplinary Policies in the Instruction of the Minister of Home Affairs No. 15 of 2021 in Banten. *KnE Social Sciences*, 101–113.

Susanto, H., Mardhiah, N., & Susanto, A. K. S. (2022). Crafting Strategies of Security Breaches: How Financial Technology Business Modela Work in Data-Centric Approaches. In *FinTech Development for Financial Inclusiveness* (pp. 214–234). IGI Global.

Tidke, S. K., Karde, P., & Thakare, V. (2017). Identification of Botnet hidden behind smartphone applications. *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, 420–424.

Troshchenkov, S., & Halona, I. (2024). International security system in the light of cyber threats: legal issues and prospects. *Публічне Управління і Політика*, *1*, 63–72. https://doi.org/10.70651/3041-2498/2024.1.07

Wahyudi, D. (2013). Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime Di Indonesia. *Jurnal Ilmu Hukum Jambi*, *4*(1), 43295.

Wiryawan, D., Suhartono, J., Fernando, Y., So, I. G., & Gui, A. (2019). Malware Mobile Devices in Indonesia. *KnE Social Sciences*, 259–267. https://doi.org/10.18502/KSS.V3I22.5055

Zakaria, S. N., & Zolkipli, M. F. (2021). Review on mobile attacks: Operating system, threats and solution. *Borneo International Journal EISSN 2636-9826*, *4*(2), 8–16.