International Conference Restructuring and
Transforming Law 2024
Volume 3, Issue 1, September 2024
e-ISSN :2963-931X
icrtlaw@ums.ac.id

THE PHENOMENON OF THE SPREAD OF RANSOMWARE VIRUS THAT INFECTS BANK SYSTEMS AND LEGAL PROTECTION FOR VICTIMS AFFECTED BY RANSOMWARE ATTACKS

Satria Dwi Andyka
Law Study Program, Faculty of Law, Universitas Muhammadiyah Surakarta
c100202318@student.ums.ac.id

Wardah Yuspin
Law Study Program, Faculty of Law, Universitas Muhammadiyah Surakarta
wy204@ums.ac.id

ABSTRACT

This research aims to understand the cases of Ransomware attacks within the banking sector. Rapid technological advance have significantly impacted the digital word, especially banking. The prevalence of Ransomware cases continues to increase each year due to the ineffectiveness of specific legal regulations governing ransomware cases. Additionally, there is a lack clarity regarding legal protection for victims affected by ransomware attacks. This study employs a normative juridical approach. Two sources of data are utilized: primary data source and secondary data. When viewed from Philipus M Hadjon's theoretical perspective, the research findings indicate ineffectiveness as it fails to fulfill other more general or universally applicable Legal Protection Theories. This implies a need for more consensus on legal protection. Many concentrates on specifics laws. This regulation of ransomware cases has not yet fully succeeded in reducing such incidents in Indonesia, as the number of cases continues to rise every year.

Keywords: Banking; Ransomware; Technology; Legal Protection

INTRODUCTION

The development of technology today is growing rapidly, technology is a means to facilitate various aspects of life, in line with the development of technology that is increasingly advanced in this modern era, there are more and more technological influences in various fields, including in the financial sector. (1)

This has a very significant impact in various sectors such as in the banking world, technological advances in the banking world have proven to have a very positive impact, namely the ease and comfort of accessing information via the internet or mobile banking, one of which is

ease of access, technology allows customers to access accounts and conduct banking transactions online via mobile devices or computers, making it easier for them to make transactions anytime and anywhere, besides the impact of technological advances in the banking world that is very useful for life at this time is *blockchain* technology where the technology is used to improve transparency, especially in terms of cross-border payments and supply chain management, in the whole technology has changed the way banks operate. Providing more efficient and convenient services to customers and increasing the security of banking transactions, but for all the convenience and comfort offered by Internet technology, especially in the banking world, there are always negative impacts that arise, such as loss of balances or theft of customer data in plain sight. Currently, there is a surge in cybercrime crimes that utilize advances in information technology, such as ATM / EDC skimming, pharming, spoofing, phishing, money laundering, online gambling, malware (viruses / worms / bots), and one of the most talked about is ransomware. Ransomware is a type of malware that works by encrypting or processing data into unreadable code, making victims unable to access data until the data is decrypted again. According to the Interpol Cyber Assessment Report 2021, approximately 2.7 million ransomware attacks were detected in Southeast Asian countries from January to September 2020. Indonesia ranked highest with 1.3 million cases, followed by Vietnam with 886,784 cases, Thailand with 192,652 cases, and the Philippines with 137,366 cases. (2)

On May 8, 2023, Indonesia was shocked by a ransomware case that hit Bank Syariah Indonesia (BSI) Services and lasted for four days until May 11, 2023. The attack managed to penetrate the bank's security system and encrypt sensitive data, including important customer and financial information. The total stolen data reached 1.5 TB, including customer personal information such as name, cellphone number, address, account balance, account number, transaction history, as well as user data and passwords for internal access and services used by customers. The impact of BSI data leakage includes exposition of customer finances that have abnormal balances, which will be of concern to the public, tax office, and authorities. This causes inconvenience and concern for customers and account owners of Bank Syariah Indonesia.

Therefore, it is important for Islamic banking institutions to implement good governance in safeguarding customer data. (3)

In addition to the ransomware case that attacked Islamic Sharia Banks, in 2022 PT Bank Pembangunan Daerah Jawa Timur (Bank Jatim) also experienced a similar incident, causing a leak of Bank Jatim customer data, in this incident it caused the sale of customer data at a price of US $ 250 thousand or IDR 3.5 billion, and there was another case of alleged BI data leaked on social media that a gang of *hackers conti ransomware* has hacked data with a capacity of 487 MB from 16 computer personnel (PCs) on January 21, 2022. (4)

The impact of ransomware attacks on Bank Syariah Indonesia, Bank Jatim, and Bank Indonesia (BI) is very serious, as it not only disrupts banking operations, but also threatens trust in the banking system and the security of their data; loss of valuable data can cause significant financial loss to customers and damage the reputation of the bank itself. The case at the Bank is a reflection that the need for serious efforts to handle ransomware cases, digital security is a priority for financial institutions and institutions that collect a lot of one's data to protect the system from damaging and harmful attacks.(5)

Previous research aims to obtain comparison and reference materials. In addition, to avoid assuming similarities with this study. Therefore, in this literature review, researchers include the results of previous research.

Irfan Arief Kurniawan, Hadi Mahmud &; Norma Dewi, (2021) in his research entitled "The Spread of WannaCry Ransomware Virus Based on Law No. 11 of 2008". This research uses the descriptive-analytical literature review method. The similarity of this study is that both discuss the spread of ransomware viruses and use the approach of Law No. 11 of 2008. The difference in this study conducted by Irfan Arief Kurniawan, Hadi Mahmud & Norma Dewi is more focused on laws governing ransomware, while this study discusses several laws and refers more to ransomware viruses in the banking world.

Nur Syamsi Tajriyani (2021) in a study entitled "Criminal Responsibility for Extortion Crimes with the Modus Operandi of Spreading Cryptolocler Ransomware". This study uses doctrinal research methods. The similarity of this study is the same as discussing the regulations

regarding the criminal act of spreading ransomware virus. The difference in this study conducted by Nur Syamsi Tajriyani is more focused on the criminal responsibility of the perpetrators of spreading ransomware viruses, while this study focuses more on how to regulate the victims affected by ransomware in the banking world.

Desyanti Suka Asih K.Tus (2021) in her research entitled "Legal Protection for Victims of Ransomware Attacks". This study used normative juridical method. The similarity of this study discusses the protection for victims affected by ransomware attacks. The difference in research conducted by Desyanti Suka Asih K.Tus focuses more on how legal protection for victims of ransomware attacks is universal, while this research focuses more on protecting the data of victims affected by ransomware attacks in the banking world.

RESEARCH METHODS

This research uses a normative juridical approach method by collecting data by studying theories, concepts and laws and regulations. With this type of descriptive research, describe a symptom and events that have occurred to date. The source of the data taken in writing this article is secondary data obtained by literature study examining legal materials which are primary legal materials such as Law No. 1 of 2023 Criminal Code article 482 concerning the criminal act of extortion with threats. Law No. 19 of 2016 concerning amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions, Law No. 27 of 2022 concerning personal data protection (PDP Law). And legal materials *skunder* through journals, opinions of legal scholars, and scientific books. Data collection techniques, namely primary law and *skunder* law, are collected through literature study and then take relevant theories, legal principles, and principles. The qualitative data analysis method includes the exposure of real cases or events that have been studied before.

RESULT AND DISCUSSION

Settings of customer data affected by ransomware on bank systems

The rapid development of technology and people's lifestyles brings rapid changes to their technological needs, here digital technology is the main choice. At present technological developments have entered the banking world, there are many positive impacts of technology in the banking world, one of which is the ease of transactions anywhere and anytime.(6)

Although technology has brought many improvements in the banking world, there are also many negative impacts that must be considered, one of which is the entry of ransomware viruses. Ransomware can spread through a variety of means, including emails containing malicious attachments, fake websites, or exploitation of software flaws. These attacks can target the devices of individuals, Companies or even Government agencies. However, the case of ransomware attacks that often occur and are used as targets is in the banking system. According to Bitfander's report, the spread of ransomware in 2021, there was a 1000% increase in ransomware attacks targeting banks. (7)

Ransomware is a form of extortion crime in cyberspace. Ransomware attacks involve encrypting data that is on a computer or device, and the perpetrators of these attacks demand a ransom in the form of money for the decryption key to be given to the victim. In many cases, this can be considered an act of extortion because ransomware actors threaten to damage or eliminate the victim's data if the data is not paid. This kind of extortion is illegal in almost all jurisdictions and it is against the law. It can be concluded that ransomware cases include extortion, threats, theft and dissemination of personal data. Where the crime is regulated in Law Number 1 of 2023 is listed in Article 482 of the Criminal Code (KUHP) concerning the criminal act of extortion and threats.

According to the guidelines of Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning electronic information and transactions. Article 26 paragraph (1), The use of any information through electronic media that concerns a person's personal data must be carried out with the consent of the person concerned unless stipulated by laws and regulations.

Threats and impacts arising from weak personal data protection can have a negative impact on banking developments such as loss of customer trust in banking institutions. If customers feel that their personal data is not secure, they may be reluctant to use digital banking services or store their personal information in banks, threats to personal data security increase the risk of fraud and identity theft. Identity theft in ransomware cases, if customer data is accessed by unauthorized parties, this can result in financial losses and harm banking reputation, significant data security breaches, banking institutions can face lawsuits from victims who feel aggrieved. These demands can result in substantial financial losses.

Bank Indonesia Regulation Number 19/12/PBI/2017 concerning the Implementation of Information Security at Bank Indonesia "If a ransomware attack occurs in the banking sector, this regulation becomes relevant because it regulates information security in banks".

Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), one of the laws that regulates the protection of personal data for one case, for example, bank customers affected by Ransomware attacks.(8) Especially in article 67 paragraph (1) confirms that it is prohibited for any person who unlawfully obtains or collects personal data that can harm other parties with a maximum prison sentence of five years and/or a maximum fine of five hundred billion rupiah. If viewed from the existence of hacked personal data and causing losses to other parties, then criminal acts through Ransomware have relevance to the provisions of article 67 paragraph (1) of the PDP Law. The next legal problem is that the sanctions provisions in article 482 of the Criminal Code with a maximum imprisonment of four years and a fine of three hundred million rupiah, as well as articles 26 paragraph (1), 27 paragraph (4), 45 paragraph (4) of the Electronic Information and Transaction Law which affirm a six-year prison sentence and a maximum fine of one billion rupiah.(9)

Legal protection for customer personal data stolen through ransomware

The increasing prevalence of electronic media as a means of communication has the potential to facilitate violations of privacy, particularly in the form of breaches or theft of personal

data. This is shaped by the behaviors and cultural norms of individuals who are inclined to share data and information.

The protection of personal data is inextricably linked to the concept of privacy. Privacy, in essence, is the notion of upholding the integrity and dignity of each individual. As the entity responsible for the management of consumer data, the company bears the obligation to ensure the security of this information against any potential breaches. The dissemination of consumers' personal data constitutes a violation of their right to privacy. It is thus evident that comprehensive legal regulations are required to safeguard consumer personal data collected by corporations. The legal provisions related to the protection of personal data are still partial and sectoral. This appears to be an obstacle to providing optimal and effective protection of personal data as part of the broader concept of privacy. The current legal framework for data protection in Indonesia is comprised of several pieces of legislation, including Law Number 27 of 2022 concerning personal data protection (PDP Law), Law Number 10 of 1998 concerning Banking, which regulates the handling of personal data pertaining to depository customers and their deposits, and Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions.(10)

The overall arrangements in tackling the above misuse of personal data, especially with respect to personal data are currently in the process of convergence. This concept elucidates the process or effort to consolidate the disparate arrangements regarding personal data dispersed across various legal instruments into a unified legal instrument. The current state of regulation regarding personal data in Indonesia is not one of convergence, but rather a state of divergence. This convergence of privacy and personal data protection does not only occur in Indonesia, but also spread in various parts of the world, without exception in the scope of countries and international organizations.

The provisions regarding the policy of handling personal data by providing protection are mandated by Article 28 G of the Constitution of the Republic of Indonesia Year 1945 (UUD) which regulates the right to protection of self, family, honor, dignity, and property under its control. To be able to see these provisions as provisions regarding privacy and personal data, Warren and

Brandeis opinion in their work entitled *"The Right to Privacy"* states that privacy is the right to enjoy life and the right to respect feelings and thoughts. This is in accordance with the Theory of Legal Protection. The theory of legal protection that develops or is often used is the Theory of Legal Protection from Philipus M Hadjon with his book entitled Legal Protection for the People. I do not think there is yet another Theory of Legal Protection that is more general or generally accepted. That is, no one has expressed an opinion about legal protection that does not focus on certain laws. Because many have expressed the theory of legal protection but focused on certain laws, such as Consumer Protection Law, Legal protection of witnesses, Child Protection, Protection of Intellectual Property Rights, and others. All of these theories always refer to Philip's Theory of Legal Protection more specifically to certain laws, so there is also no understanding of legal protection that is general or generally accepted. (11) The right to privacy and personal data is a right that has an international character in the unclear status of national legal protection.

The protection of personal data against ransomware attacks necessitates the implementation of a multifaceted approach, comprising technical measures, security policies, and individual awareness. Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) provides a legal framework that offers protection for individuals who utilize personal data, particularly for those engaged in business activities. Prior to engaging in business activities, there is a heightened susceptibility to data breaches, particularly in the context of financial transactions. These transactions can be vulnerable to exploitation by cybercriminals, who may engage in economic activities aimed at facilitating data leakage incidents. In general, the judicial process of a criminal act is based on the Criminal Procedure Code as a procedural law that contains the rules for the process of solving or handling criminal cases contained in the Criminal Code, ranging from investigation, investigation, prosecution, trial, examination events, appeal, cassation, and judicial review. The Criminal Procedure Code and the Criminal Code itself are *lex generalu* in criminal law. This means that if there are other laws outside the Criminal Procedure Code and the Criminal Code that have special procedural laws and specific criminal sanctions, then these provisions apply in a specialist manner.

Two points of contention emerge when considering the protection of national law. Privacy, on the one hand, is a right that establishes a separation between individuals and society. The Law of the Republic of Indonesia No. 19 of 2016 concerning Amendments to Law of the Republic of Indonesia Number 11 of 2011 concerning Electronic Information and Transactions (hereinafter referred to as the "ITE Law") includes provisions for protection from unauthorized use, protection by electronic system operators, and protection from illegal access. Related to tackling personal data theft through penal means, namely by providing protection to personal data from unauthorized use or utilization. Article 26 of the Electronic Information and Transaction Law requires that the use of any personal data in an electronic media must first obtain the consent of the owner of the data concerned. Any person who violates this provision may be sued for damages caused.

In its explanation, Article 26 of the Electronic Information and Transaction Law also states that personal data is one part of a person's personal rights. Law of the Republic of Indonesia Number 19 of 2016 Amendments to Law of the Republic of Indonesia Number 11 of 2011 concerning Electronic Information and Transactions as a generic Law contains personal data protection norms in Article 26, which in essence, the use of any data and information in electronic media related to a person's personal data must be carried out with the consent of the person concerned or based on the current positive law (laws and regulations). Basically, this provision contains two bases for the legitimacy of processing personal data, namely (a) consent; and (b) positive legal norms. These two principles are the basis of lawful data processing.(12)

Based on the content of the articles above, it means that activities such as collecting and disseminating personal data are violations of a person's privacy because privacy rights include the right to determine whether or not to provide personal data. Including the theft of personal data, when electronic operators use personal data belonging to others, the form of prohibition is none other than the government's view that personal data is an asset or commodity of high economic value.

CONCLUSION

Legal provisions related to personal data protection are still partial and sectoral, it seems that they have not been able to provide optimal and effective protection for personal data, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) has not proven effective because it does not provide adequate protection for the rights of personal data subjects. A personal data subject is an individual whose personal data is collected, processed, or regulated by an organization or system, such as in a banking context. Despite the existence of regulations pertaining to the protection of personal data, instances of data theft remain a prevalent phenomenon. This is evidenced by the prevalence of ransomware attacks, which have become a significant concern in recent times. This indicates that the implementation of the PDP Law has not been wholly effective in addressing this issue. Based on the theory presented by Philipus M. Hadjon regarding legal protection, namely the protection of human rights and dignity, as well as recognition of human rights, it can be seen that the PDP Law has not been able to fulfill the human rights of personal data subjects.

In the Electronic Information and Transaction Law, especially Article 26, the government provides a solution when electronic system operators violate personal data by allowing civil lawsuits in court. To prevent personal data breaches and theft, the Electronic Information and Transaction Law requires electronic system operators to make adjustments and deletions of inappropriate personal data based on court requests. However, the deletion process is still vague, only mentioning the removal of irrelevant information without detailed explanation. This is potentially contrary to other laws, such as the Press Law and Public Information Openness. However, the Electronic Information and Transaction Law regulations related to personal data are still not comprehensive, including the scope of protection, the definition of sensitive data, and the difficulty of proof in civil courts, making it difficult for data owners to legally prosecute theft or leakage of personal data. Philipus M Hadjon stressed the importance of legal protection to ensure individual rights are protected, including in personal data protection laws.

REFERENCES

1. Dwididanti S, Anggoro DA. Analisis Perbandingan Algoritma Bisecting K-Means dan Fuzzy C-Means pada Data Pengguna Kartu Kredit. Emitor: Jurnal Teknik Elektro. 2022 Aug 14;22(2):110–7.
2. Vika Azkiya Dihni. databoks. 2022 [cited 2024 May 5]. Indonesia Alami Kasus Serangan Ransomware Terbanyak di Asia Tenggara. Available from: https://databoks.katadata.co.id/datapublish/2022/06/08/indonesia-alami-kasus-serangan-ransomware-terbanyak-di-asia-tenggara
3. Purbasari H, Puspawati D. Exploration Study of Sharia Corporate Exploration Study of Sharia Corporate Governance Disclosure on Bank Annual Governance Disclosure on Bank Annual Report of Sharia Business Unit Report of Sharia Business Unit [Internet]. Available from: http://journals.ums.ac.id/index.php/reaksi/index
4. Tasman T UU. UNES LAW REVIEW. Perlindungan Hukum Terhadap Nasabah Bank Digital . 2023 Sep 20;6(01).
5. Hartono B. Ransomware: Memahami Ancaman Keamanan Digital. Bincang Sains dan Teknologi. 2023 May 21;2(02):55–62.
6. TRANSFORMASI DIGITAL PERSIDANGAN DI ERA NEW NORMAL [Internet]. Available from: www.imajimedia.com
7. Redaksi. CNBC Indonesia. 2023 [cited 2024 May 5]. Banyak Bank Jadi Target Serangan Ransomware, Kenapa? Available from: https://www.cnbcindonesia.com/tech/20230515122147-37-437351/banyak-bank-jadi-target-serangan-ransomware-kenapa
8. Persetujuan Bersama D. FRESIDEN REPUBLIK INDONESIA 2-DEWAN PERWAKILAN RAKYAT REPUBLIK INDONESIA dan PRESIDEN REPUBLIK INDONESIA.
9. Aziziyah T, Purwoleksono DE, Rachman T. Sniffing Cybercrimes in M-Banking via WhatsApp: Comparative Legal Framework and Implications. Rechtsidee. 2023 Dec 2;12(2).
10. Jurnal+Jofani+Maramis-1.

11. Mu'in F, Oktavianda B, Martinouva RA, Muliawan C. PERLINDUNGAN HUKUM KONSUMEN DALAM TRANSAKSI BISNIS FINTECH PADA PT. LAMPUNG BERKAH FINANSIAL TEKNOLOGI.
12. UNDANG-UNDANG REPUBLIK INDONESIA.