**ICCCM-JOURNAL OF SOCIAL SCIENCES AND HUMANITIES**
2024; 3(2): 26-32
Published online 03 06 2024 ( https://icccmjssh.com/ )
https://doi.org/10.53797/icccmjssh.v3i2.6.2024
e-ISSN 2811-4469

# Theft of Customer Personal Data as a Cybercrime in the Banking Sector

## Khofifah

Department of Law, Universitas Muria Kudus, Kudus, 59327 Central Java, Indonesia

*Corresponding author: 202202028@std.umk.ac.id

**To Cite This Article:**

Khofifah. (2024). Theft of Customer Personal Data as a Cybercrime in the Banking Sector. *ICCCM Journal of Social Sciences and Humanities, 3*(2), 26–32. https://doi.org/10.53797/icccmjssh.v3i2.6.2024

**Abstract:** One of the technological developments that can be felt by society today is the advancement of information technology in the banking sector. The development of banking technology makes it easier for customers to transact with each other. However, this rapid technological development can lead to cybercrimes in the banking sector, such as theft of customer personal data. Customer personal data is important and must be protected based on the principle of banking secrecy. Cybercrimes in the banking sector that are capable of being carried out for various banking activities are related to the security system when carrying out each activity. The theft of customer personal data has become a problem for society due to technological developments. The purpose of this research is to find out the law enforcement for the perpetrators of customer personal data theft and to find out the punishment given to the perpetrators of customer personal data theft. The method used in this research is the normative juridical method, namely research based on literature related to law enforcement for perpetrators of customer personal data theft. Law enforcement in this case must be carried out optimally so that people feel safe and protected from cybercrime. Criminal liability for perpetrators of customer personal data theft is carried out as a law enforcement of customer personal data theft. Law enforcement of personal data is carried out based on law number 11 of 2008 concerning information and electronic transactions (ITE) and law number 27 of 2022 concerning on personal data protection.

**Keywords:** Cyber-crime, theft of customer personal data, law enforcement, banking sector

## 1. Introduction

One form of information technology development that can be felt by the community today is the increase in information systems in the banking sector. Banks as one of the financial institutions have a big role in the economy of the community (Xiong et al., 2017). banks act as a form of financial institution that aims to provide funds or other services and the provision of funds is carried out by circulating means of payment in the form of demand deposits (Yusuf, 2022). In the current era of globalization, Banks are part of a country's payment system. if a bank has obtained a license to stand and operate from the monetary authority of the country concerned, then the bank has become the property of the Community, so that its existence must be maintained by bank owners and the wider community (Ratulangi et al., 2021).

As a place of money circulation, banks have a position that is vulnerable to abuse of authority and is used as a place to hide the results of crime by the bank itself or by outsiders. For example, there are banking activities that have certain motives so that they exceed or do not comply with applicable regulations, so this is referred to as banking crime or banking crime (Statesenko et al., 2019). The banking crime is carried out in relation to the security system in carrying out each of its activities (Sulisrudatin, 2014). Nowadays technology is considered a force and power that determines the fate of humans themselves. Society's dependence on information technology is getting higher so that the risks faced are also getting higher (Rumlus & Hartadi, 2020). Therefore, the public is urged to always be vigilant and careful in using technology in this era of globalization.

Chapter 4 of Law Number 11 of 2008 concerning Information and Electronic Transactions explains the purpose of utilizing information technology and electronic transactions, are: 1) to educate the nation's life as part of the world information society; 2) develop trade and the national economy in order to improve people's welfare; 3) improving the effectiveness and efficiency of public services; 4) to open the widest possible opportunity for every person to advance their thoughts and abilities in the field of the use and utilization of Information Technology as optimally as possible and responsibly; and 5) provide a sense of security, justice, and legal certainty for users and organizers of information technology. Information technology is a double-edged sword because in addition to contributing to the improvement of

**Corresponding author: 202202028@std.umk.ac.id*
*https://icccmjssh.com/* All right reserved.

welfare, progress and human civilization, information technology is also an effective means of unlawful acts. These various forms of crime are called "cybercrime" (Rumlus & Hartadi, 2020).

One of the problems arising from the development of information technology is the birth of new crimes, especially those that use the internet as a tool or cybercrime, such as hackers, crackers, cybersquating, and others. Ways that can be done by destroying data, stealing data, and using it illegally and this is done by someone who controls and is able to operate computers such as operators, programmers, analysts, consumers, managers, and a cashier. Other examples of cybercrime include infringement of intellectual property rights, slander or libel, violation of privacy, threats and extortion, sexual exploitation of children and sexual abuse, tampering with computer systems, breaking access codes, and forgery of digital signatures (Bahrudin & Hidayatullah, 2021; IIchenko et al., 2019). Cybercrime can also take the form of data falsification, spreading computer viruses to computer networks or computer systems, adding or subtracting system instructions in computer networks, rounding numbers, destroying data, and leaking confidential data (Farwansyah, 2022). cybercrime is currently widespread, and most of it occurs in the banking sector such as the theft of personal data of Bank Syariah Indonesia customers.

The development of the internet is not entirely beneficial for the people of Indonesia. There are times when internet development becomes something that is not useful and becomes a problem for the community, namely related to the theft of personal data. Personal data theft is one of the links between the development of information technology and the law, especially criminal law. The relationship between criminal law and the development of information technology in Indonesia, criminal law becomes a coercive tool for users of information technology so that it does not cause harm to everyone who uses it (Benuf, 2021). personal data is protected by security systems and laws and regulations. if there are people who commit unlawful acts related to personal data, then they can be sentenced according to what they have done.

The rapid development of the internet makes it difficult for the government to handle cybercrimes if it relies on conventional positive law. Although the law has an important role in preventing and overcoming crime, creating legal regulations that are in accordance with the rapid development of information technology is not easy. Therefore, legal regulations often become outdated quickly when regulating things that are constantly changing, resulting in a legal vacuum. This is also the case in dealing with cybercrime (Yudistira & Ramadhan, 2023). Cybercrime must be anticipated and also addressed with a legal umbrella that has a relationship with the world of information technology and communication, because it guarantees legal protection for people who use information technology (Ningrum & Robekha, 2023). Of course, this is a challenge for the Government in creating new policies that are in accordance with the development of information technology.

Protection related to the use of information technology is regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions. Protection of customer personal data is important and must be protected based on the principle of banking confidentiality. Customer personal data is a privacy right that must be guaranteed protection. Customer data such as name, date of birth, mother's name, home address, email address, or cell phone number must be kept confidential by the bank (Widayanti, 2022). This is in accordance with Article 26 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, namely that unless otherwise provided by Laws and Regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned. Personal rights have the meaning of the right to have a private life and should not be disturbed, personal rights are the right to be able to communicate using with other people without being spied on, and personal rights are the right to access information about direct life and personal data (Anugerah & Tantimin, 2022).

Cybercrime in the Criminal Code is still regulated in general. The principle of Lex Specialis derogat legi Generalis means that special legislation or rules of law override general legislation or rules of law. So that with this principle in handling Cybercrime cases in the banking sector can use more specific regulations, which include in addition to Law Number 11 of 2008 concerning Electronic Information and Transactions there is also Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking, Law Number 8 of 1999 concerning Consumer Protection, Law Number 27 of 2022 concerning Protection of Personal Data. the existence of these rules, customers feel protected in the event of misuse of their personal data (Ekayani & Djanggih, 2023).

Based on the background of the problem, it can be seen that the legal substance regarding cybercrime already exists, but cybercrime cases are still unresolved until now. Therefore, from this problem, the formulation of the problem that can be raised is how the law enforcement against cybercrime of customer data theft in the banking sector? How is criminal liability for perpetrators of cybercrimes of customer data theft in the banking sector?

## 2. Methodology

The research method used is normative juridical. This method is a research method that comes from literature. This research is commonly referred to as doctrinal legal research. Often this research is conceptualized as what is written in the laws and regulations (Efendi & Ibrahim, 2018). Researchers attempt to collect and then analyze the law, along with relevant legal norms. Normative juridical legal research can be defined as research that asks whether the law in a particular jurisdiction (Tan, 2021). Juridical-normative legal research (also known as doctrinal legal research) can be interpreted simply as research that asks whether the law in a particular jurisdiction. This research uses secondary data in the form of primary legal sources, secondary legal sources and tertiary legal sources.

# 3. Results and Discussion

## 3.1 Law Enforcement Against Cyber Crimes of Customer Data Theft in the Banking Sector

The definition of cybercrime is a form of crime as a direct result of the development of information technology using the internet as a medium for committing crimes. Crimes that used to be committed when there was physical contact between the perpetrator and the victim in committing a crime then became a crime in cyberspace or cybercrime which can be committed without physical contact between the perpetrator and the victim using the internet media and other electronic devices (Juanrico et al., 2023). Crimes or criminal offenses are acts that cause suffering, so they must be prevented or overcome. However, preventing or overcoming crime is not easy or simply equalized steps for every crime (Sulisrudatin, 2014).

The most important part of society that determines law enforcement against cybercrime is public legal awareness. The higher the level of public legal awareness, the higher the level of public legal awareness, the more good law enforcement will be possible. Conversely, the lower the level of public legal awareness, the more difficult it will be to implement good law enforcement. Legal awareness includes knowledge of the law, appreciation of legal functions and obedience to the law. the bank as the main law enforcer in electronic transactions in the banking sector and the public will feel that their online transaction activities are safe as long as they are guided by the bank employees themselves so that customer knowledge regarding various cybercrimes and the importance of privacy in social networking can increase (Ekayani & Djanggih, 2023).

Theft of customer personal data is one of cybercrime. This personal data theft can be said to be a violation by breaking into an electronic system to take someone's personal data without permission, which is then used for other crimes such as fraud (Luthiya et al., 2021). As for personal data, it is a person's personal right that must not be violated. Explanation of Article 26 of Law Number 19 of 2016 Concerning the Amendment to Law Number 11 of 2008 Concerning Electronic Information and Transactions that personal rights contain the following meanings are: 1) personal rights are the right to enjoy a private life and to be free from all kinds of interference; 2) the right to privacy is the right to be able to communicate with others without spying; and 3) the right to privacy is the right to monitor access to information about one's private life and data.

According to Coteanu (2020) and Umanailo et al. (2019), cybercrime was born due to the lack of ability or knowledge of law enforcement officials in handling cybercrime cases. Other factors that cause personal data theft are: 1) unlimited internet access; 2) computer user negligence; 3) easy to do with little security and no super-modern equipment required; 4) the perpetrators are generally intelligent and curious people; 5) weak network security system; and 6) lack of community attention (Sari et al., 2021).

Law enforcement is a process to realize legal desires into reality. Law enforcement in a broad sense includes activities to implement and apply or deviations from the law by legal subjects, both through arbitration procedures and other dispute resolution mechanisms (Yusuf, 2022). Regarding human rights and personal ownership is regulated in Article 28G paragraph 1 of the 1945 Constitution of the Republic of Indonesia which explains that "Everyone has the right to protection of self, family, honor, dignity, and property under his control, and is entitled to a sense of security and protection from threats of fear to do or not do something that is a human right". So it can be said that the constitution of the Republic of Indonesia has guaranteed the right to protection of personal data owned by every person in Indonesia (Benuf, 2021).

Legal protection of personal data is an important need for every individual, and the responsibility of law enforcement to protect these basic rights. As explained in law number 27 of 2022 concerning the protection of personal data, there are: a) personal data protection is one of human rights which is part of personal protection, therefore it is necessary to provide a legal basis to provide security over personal data, based on the 1945 Constitution of the Republic of Indonesia; b) the protection of personal data is aimed at ensuring the rights of citizens to personal protection and fostering public awareness and guaranteeing recognition and respect for the importance of personal data protection; and c) the regulation of personal data is currently contained in several laws and regulations, therefore, to increase the effectiveness in the implementation of personal data protection, it is necessary to regulate the protection of personal data in a law (Yudistira & Ramadhan, 2023).

Law enforcement against the perpetrators of criminal acts of theft of banking customer data is an effort made by law enforcement officials to eradicate the perpetrators of criminal acts of theft of banking customer data that harm the state and society. Criminal law enforcement efforts in the understanding of the legal system include the operation of the components of legislation or substance, law enforcement officials or structure and legal culture or culture (Yusuf, 2022). Prevention and control of criminal acts in the context of law enforcement against customer data theft can be done in two (2) ways, there are penal and non-penal. Penal usually emphasizes on repressive efforts. Penal policy is the duty of the police, prosecutors, judges, and of course Bank Indonesia in terms of administrative violations. Meanwhile, non-penal policy is the duty of law enforcement officials, Bank Indonesia, public and private banks and the public (Lacey et al., 2018; Sulisrudatin, 2014). The role of the community here is very important in law enforcement efforts against cybercrime theft of customer data.

In reality, the law enforcement process culminates in its implementation by law enforcement officials. Law enforcement officials in Indonesia are judges, prosecutors, police. The judge is one of the law enforcement officials who

carry out a judicial system that has the task of receiving and deciding cases in a fair manner. Law enforcement will always involve humans in it and likewise human behavior is involved in it. The law cannot be upheld by itself so that it involves law enforcement officials, and the apparatus in realizing the enforcement of the law must be with laws, means, and culture, so that the law can be enforced fairly in accordance with the ideals of the law itself (Situmeang, 2020).

## 3.2 Criminal Liability for Perpetrators of Cybercrime of Customer Data Theft in the Banking Sector

Cybercrime is basically the impact of technological developments that have changed the habits of society which were originally conventional into a more modern habit or can be called a high technology society. The existence of Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 on Information and Electronics can actually increase customer security and comfort when conducting banking activities through electronic systems provided by banks (Hakim, 2018). The Theft of information or personal data not only threatens individuals, but also communities and the Indonesian people as a whole. Therefore, there is an urgent need to develop more comprehensive and specific regulations regarding personal data protection in Indonesia (Sinaga, 2023).

Criminal responsibility is a joint of the broad notion of guilt, there are three requirements regarding criminal responsibility, there are: 1) the possibility of determining one's will for an act; 2) knowing the real intent of the act; and 3) awareness that it is prohibited in society (Wibowo et al., 2021).

The application of legal sanctions against perpetrators of theft of customer personal data is contained in Law Number 11 of 2008 concerning Electronic Information and Transactions Article 30, Article 32 and Article 35, in addition to criminal provisions contained in Article 46, Article 48, Article 51.

Article 30

(1) Every person intentionally and without right or unlawfully accesses another person's Computer and/or Electronic System by any means whatsoever.
(2) Every person intentionally and without right or unlawfully accesses a computer and/or Electronic System by any means with the purpose of obtaining Electronic Information and/or Electronic Documents.
(3) Every Person intentionally and without right or unlawfully accesses a computer and/or Electronic System by any means by violating, breaking through, exceeding, or breaching the security system.

Article 32

(1) Every person intentionally and without right or unlawfully by any means alters, adds, reduces, transmits, damages, removes, moves, conceals Electronic Information and/or Electronic Documents belonging to another person or to the public.
(2) Every Person shall intentionally and without right or unlawfully by any means move or transfer Electronic Information and/or Electronic Documents to the Electronic System of another unauthorized person.
(3) For the act as referred to in paragraph (1) which results in the disclosure of confidential Electronic Information and/or Electronic Documents to be accessible to the public with data integrity that is not as it should be.

Article 35

“Every person intentionally and without rights or against the law manipulates, creates, changes, removes, destroys Electronic Information and / or Electronic Documents with the aim that the Electronic Information and / or Electronic Documents are considered as authentic data.”

Article 46

(1) Every person who fulfills the elements as referred to in Article 30 paragraph (1) shall be punished with a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp600.000.000.00 (six hundred million rupiah).
(2) Every person who fulfills the elements as referred to in Article 30 paragraph (2) shall be punished with a maximum imprisonment of 7 (seven) years and/or a maximum fine of Rp700.000.000.00 (seven hundred million rupiah).
(3) Every person who fulfills the elements as referred to in Article 30 paragraph (3) shall be punished with a maximum imprisonment of 8 (eight) years and/or a maximum fine of Rp800.000.000.00 (eight hundred million rupiah).

Article 48

(1) Every person who fulfills the elements as referred to in Article 32 paragraph (1) shall be punished with a maximum imprisonment of 8 (eight) years and/or a maximum fine of Rp2.000.000.000.00 (two billion rupiah).
(2) Every person who fulfills the elements as referred to in Article 32 paragraph (2) shall be punished with a maximum imprisonment of 9 (nine) years and/or a maximum fine of Rp3.000.000.000.00 (three billion rupiahs).
(3) Every person who fulfills the elements as referred to in Article 32 paragraph (3) shall be punished with a maximum imprisonment of 10 (ten) years and/or a maximum fine of Rp5.000.000.000.00 (five billion rupiah).

Article 51

(1) Every person who fulfills the elements as referred to in Article 35 shall be punished with a maximum imprisonment of 12 (twelve) years and/or a maximum fine of Rp12.000.000.000.00 (twelve billion rupiahs).
(2) Every person who fulfills the elements as referred to in Article 36 shall be punished with a maximum imprisonment of 12 (twelve) years and/or a maximum fine of Rp12.000.000.000.00 (twelve billion rupiahs).

In addition to using the provisions of Law Number 11 Year 2008, perpetrators of customer data theft can also be sentenced in Law Number 27 Year 2022 on Personal Data Protection Article 65, Article 66, while criminal provisions are contained in Article 67, Article 68.

Article 65

(1) Every Person shall be prohibited from unlawfully obtaining or collecting Personal Data that does not belong to him/her with the intention to benefit himself/herself or another person which may result in harm to the Personal Data Subject.
(2) Every Person is prohibited from unlawfully disclosing Personal Data that does not belong to him/her.
(3) Every person is prohibited from unlawfully using Personal Data that does not belong to him/her.

Article 66

"Every Person is prohibited from creating false Personal Data or falsifying Personal Data with the intention to benefit themselves or others which may result in harm to others."

Article 67

(1) Any Person who intentionally and unlawfully obtains or collects Personal Data that is not his/her own with the intention to benefit himself/herself or another person which may result in harm to the Personal Data Subject as referred to in Article 65 paragraph (1) shall be punished with a maximum imprisonment of five (5) years and/or a maximum fine of Rp5.000.000.000.00 (five billion rupiahs).
(2) Every Person who intentionally and unlawfully discloses Personal Data that does not belong to him/her as referred to in Article 65 paragraph (2) shall be punished with a maximum imprisonment of four (4years and/or a maximum fine of Rp4.000.000.000.00 (four billion rupiahs).
(3) Every person who intentionally and unlawfully uses Personal Data that does not belong to him as referred to in Article 65 paragraph (3) shall be punished with a maximum imprisonment of five (5) years and/or a maximum fine of Rp5.000.000.000.00 (five billion rupiahs).

Article 68

"Any Person who intentionally creates false Personal Data or falsifies Personal Data with the intent to benefit themselves or others which may result in harm to others as referred to in Article 66 shall be punished with a maximum imprisonment of six (6) years and/or a maximum fine of Rp6.000.000.000.00 (six billion rupiahs)."

## 4. Conclusion

Based on this research, it can be concluded that law enforcement efforts to implement and apply or deviations from the law by legal subjects, both through arbitration procedures and other dispute resolution mechanisms. Law enforcement against the perpetrators of criminal acts of theft of banking customer data is an effort made by law enforcement officials to eradicate criminal acts of theft of banking customer data that harm the state and society. This enforcement needs to involve law enforcement officials, and officials in realizing the rule of law must be with laws, means, and culture, so that the law can be enforced fairly in accordance with the ideals of the law itself.

The application of legal sanctions against perpetrators of customer personal data theft is contained in Article 30, Article 32 and Article 35, Article 46, Article 48, Article 49, Article 51 of Law Number 11 of 2008 concerning Electronic Information and Transactions. In addition to using the provisions of Law Number 11 of 2008, perpetrators of customer data theft can also be sentenced in Article 65, Article 66, Article 67, Article 68 of Law Number 27 of 2022 concerning Personal Data Protection.

## References

Anugerah, F., & Tantimin, T. (2022). Pencurian Data Pribadi Di Internet Dalam Perspektif Kriminologi. *Jurnal Komunikasi Hukum (JKH)*, *8*(1), 419–435. https://doi.org/10.23887/jkh.v8i1.45434

Bahrudin, B., & Hidayatullah, H. (2021). PKPU Policy Number 20 of 2018 Concerning the Prohibition of Former Corruptors as Legislative Candidates in the 2019 General Election. *KnE Social Sciences*, *2021*(20), 13–21. https://doi.org/10.18502/kss.v5i7.9315

Benuf, K. (2021). Hambatan Formal Penegakan Hukum Pidana Terhadap Kejahatan Pencurian Data Pribadi. *Majalah Hukum Nasional*, *51*(2), 261-279. https://doi.org/10.33331/mhn.v51i2.148

Coteanu, C. (2020). Cyber law, Cyber Consumer Law and Unfair Trading Practices, *Computer Law & Security Review*, *23*(1), 83. https://doi.org/10.1016/j.clsr.2006.10.006

Efendi, J., & Ibrahim, J. (2018). *Metode Penelitian Hukum Normatif dan Empiris*. Depok: Prenada Media.

Ekayani, L., & Djanggih, H. (2023). Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi (Phising) Di Lingkungan Perbankan. *Journal of Lex Philosophy (JLP)*, *4*(1), 22-40. https://doi.org/10.52103/jlp.v4i1.1485

Farwansyah, A. (2022). *Penegakan Hukum Tindak Pidana Pencurian Data Kartu Kredit (CARDING) Di Wilayah Hukum Kepolisian Daerah Riau* (Doctoral dissertation, Universitas Islam Riau).

Hakim, L. (2018). Pertanggungjawaban Lembaga Perbankan terhadap Pencurian Data Nasabah. *Dialogia Iuridica: Jurnal Hukum Bisnis dan Investasi*, *10*(1), 01-15. https://doi.org/10.28932/di.v10i1.918

Ilchenko, O., Chumak, V., Kuzmenko, S., Shelukhin, O., & Dobrovinskyi, A. (2019). Fishing as a cybercrime in the Internet banking system: economic and legal aspects. *J. Legal Ethical & Regul. Isses*, *22*, 1.

Juanrico, A. S. ., Rinaldi, K., Atikah, I., & Mustafa, L. O. A. (2023). *Hukum Cyber* (Vol. 01). Penerbit Widina Media Utama.

Lacey, N., Soskice, D., & Hope, D. (2018). Understanding the determinants of penal policy: Crime, culture, and comparative political economy. *Annual Review of Criminology*, *1*, 195-217. https://doi.org/10.1146/annurev-criminol-032317-091942

Luthiya, A. N., Irawan, B., & Yulia, R. (2021). Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi. *Jurnal Hukum Pidana dan Kriminologi*, *2*(2), 14-29. https://doi.org/10.51370/jhpk.v2i2.43

Ningrum, D. P. S., & Robekha, J. (2023). Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking di Indonesia. *PESHUM: Jurnal Pendidikan, Sosial Dan Humaniora*, *2*(4), 765-776. https://doi.org/10.56799/peshum.v2i4.2115

Ratulangi, C. H. (2021). Tindak Pidana Cyber Crime Dalam Kegiatan Perbankan. *Lex Privatum*, *9*(5), 179–187. *Scribbr.* https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/33510

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan penanggulangan pencurian data pribadi dalam media elektronik. *Jurnal Ham*, *11*(2), 285-299. http://dx.doi.org/10.30641/ham.2020.11.285-299

Sari, M. P., Mamang, D., & Zakky, M. (2021). Penegakkan Hukum terhadap Tindak Pidana Pencurian Data Pribadi melalui Internet Ditinjau dari Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE (Informasi dan Transaksi Elektronik). *Jurnal Hukum Jurisdictie*, *3*(2), 1–12. https://doi.org/10.34005/jhj.v3i2.44

Sinaga, H. (2023). Legal and Ethical Implications in Data Theft Cases in the Digital Era. *East Asian Journal of Multidisciplinary Research*, *2*(11), 4585–4604. https://doi.org/10.55927/eajmr.v2i11.6791

Stetsenko, S., Syniavska, O. Y., Shelukhin, M. L., Lukash, S., & Barash, Y. (2019). Financial and legal regulation of electronic money circulation in developed countries. *J. Legal Ethical & Regul. Isses*, *22*, 1.

Sulisrudatin, N. (2014). Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit. *Jurnal Ilmiah Hukum Dirgantara*, *9*(1), 26–39. https://doi.org/10.35968/jh.v9i1.296

Tan, D. (2021). Metode Penelitian Hukum: Mengupas dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, *8*(8), 2463–2478. *Scribbr.* http://jurnal.um-tapsel.ac.id/index.php/nusantara/article/view/5601

Umanailo, M., Fachruddin, I., Mayasari, D., Kurniawan, R., Agustin, D. N., Ganefwati, R., ... & Hallatu, T. G. R. (2019). Cybercrime case as impact development of communication technology that troubling society. *International Journal of Scientific & Technology Research*, *8*(9), 1224-1228. *Scribbr.* http://repository.iainkediri.ac.id/id/eprint/630

Wibowo, S. A., Syahrin, A., & Mulyadi, M. (2021). Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan Dengan Metode Skimming Di Tinjau Menurut Undang-Undang Informasi Dan Transaksi Elektronik. *Iuris Studia: Jurnal Kajian Hukum*, *2*, 138–143. https://doi.org/10.55357/is.v2i2.100

Widayanti, P. W. (2022). Tindak Pidana Pencurian Data Nasabah Dalam Bidang Perbankan Sebagai Cyber Crime. *Legacy: Jurnal Hukum Dan Perundang-Undangan*, *2*(2), 1-21.

Xiong, W., Fu, H., & Wang, Y. (2017). Money creation and circulation in a credit economy. *Physica A: Statistical Mechanics and its Applications*, *465*, 425-437. https://doi.org/10.1016/j.physa.2016.08.023

Yudistira, M., & Ramadani, R. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 oleh KOMINFO. *UNES Law Review*, *5*(4), 3917-3929. https://doi.org/10.31933/unesrev.v5i4.698

Yusuf, M. (2022). Penegakan Hukum Bagi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan Menurut Undang–Undang Informasi dan Transaksi Elektronik. *National Journal of Law*, *6*(1), 804-818. https://doi.org/10.47313/njl.v6i1.1682