**LEGAL BRIEF**
ISSN 2722-4643 (Online) | 1979-522X (Print)
Volume 13, No.2, 2024, pp. 246-254
Published by: IHSA Institute (Natural Resources Law Institute)

# Customer Data Protection by Bank Rakyat Indonesia is Reviewed by Law Number 27 of 2022 Concerning Personal Data

**Della Gatiko Negoro[1], Gunawan Hadi Purwanto[2]**

[1,2] Universitas Bojonegoro

**Abstract:**This research aims to determine the suitability of Bank Rakyat Indonesia's form of personal data protection for customers in accordance with Law Number 27 of 2022 concerning Personal Data Protection. Individuals and community groups take advantage of the lack of boundabetween public space and privacy to operate and seek profits via the Internet, giving birth to a phenomenon known as cybercrime, one of which is the violation and theft of personal infor-The research method used is normative-empirical legal research. Data sources come from primary legal materials and secondary legal materials. Qualitative data analysis techniques are presented descriptively. The result is that the right to privacy is part of human rights which is specifically protected by the Personal Data Protection Law no. 27 of 2022 as a response to developments in technology, information and communication. The aim of enacting the Personal Data Protection Law Number 27 of 2022 is to protect and guarantee the basic rights of citizens in protecting the privacy of personal data. Then, the substantive framework of the Personal Data Protection Law Number 27 of 2022 is also in line with the right to privacy and the values contained in the philosophy of Indonesian society. Law Number 27 of 2022 concerning Personal Data Protection is expected to guarantee comprehensive protection and prevent illegal activities against the personal data of Indonesian citizens.

**Keywords:**Customer, Bank Rakyat Indonesia, Personal Data

## 1. Introduction

The phenomenon of the development of information and communication (ICT) which is in line with globalization that is occurring in the Industrial Revolution 4.0 era has greatly influenced the lives of Indonesian people.(Santoso, 2006). Even though it is largely synonymous with economic development, it also has a very important influence outside the economic field, such as politics, culture, law, and even state ideology.(Hasan & Azis, 2018),(Danil, 2021). On a national scale, the development of information and communication technology (ICT) has greatly influenced the increasingly dynamic lifestyle of Indonesian society. With ICT, access anywhere in the world is unlimited, meaning anyone can access anything via a network connected to the Internet(Khansa & Putri, 2022),(Hariyadi, Misnawati, & Yusrizal, 2023). As a form of innovation, ICT can now carry out the functions of collecting, storing, sharing and analyzing information optimally(Tasyah et al., 2021),(Iskandar, 2020).

The development of appropriate technology makes it possible to fulfill various needs without distance or time(Marfai, 2019),(Pujiono, 2021). With the help of technology, processes can be simplified, time can be shortened and the budget required to carry out activities can be reduced(Azwir, Wijaya, & Oemar, 2021) (Rini & Harahap, 2021). Indonesian society has implemented and utilized various activities such as the application of electronic business (e-commerce) in the field of trade/business, the application of electronic education (e-education) in the field of education, the application of e-Government in public administration, search engines from a search perspective information, social networks from the perspective of interaction, the development of the smartphone and mobile Internet industries, and the development of the cloud computing

**Correspondence:**
*Della Gatiko Negoro*
*dellabojonegoro813@gmail.com*

Received:May 02, 2024;
Revised:May 13, 2024;
Accepted:Jun 06, 2024;
Published:June 30, 2024

industry(Haryaningsih & Juniwati, 2021),(Yunita et al., 2023).

The important role of information technology influences the transformation of the information technology system itself for various business needs, including banking companies. Banking companies respond quickly to developments in information technology systems, continuing to offer services that make it easier for customers to access information using advanced information technology(Saputra, Kharisma, Rizal, Burhan, & Purnawati, 2023),(Putri et al., 2022). Banks use online media as a new tool to achieve customer satisfaction in service development. Information technology-based banking services are known as electronic banking or abbreviated as E-banking(Nursakinah, 2020). Internet banking services are services that help customers complete payment transactions such as bank transfers, BPJS (Social Security Agency) payments, shopping, checking account balances, and so on.(Narew & Irmawati, 2022).2 Bank Rakyat Indonesia also strives to continue carrying out digital transformation by providing access to banking services. This can be seen in 2022, financial transactions via Bank Rakyat Indonesia Internet banking will approach IDR 2.669 billion, a double increase compared to last year, and the number of transactions will reach up to 1.83 billion transactions. As a result, the number of online banking users increased by 68.46% compared to the previous year to reach 23.85 million users in December 2022(Ni'mah, Awaluddin, & Sijal, 2022).

The positive impact of technological developments does not only happen like this, but there are also other parties with bad intentions who seek profit through crime. As stated in the General Explanation of Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions, information technology is now a double-edged sword because it not only improves the welfare, growth and civilization of citizens, but also serves as an efficient means of action against the law.(Fitri, 2022),(Anggriani & Arifin, 2019).

Individuals and societal groups have taken advantage of the lack of interactive boundaries between public space and privacy to operate and seek profits via the Internet, giving rise to a phenomenon known as cybercriminals. Misuse of information and communication technology (ICT) in the field of data and information management is likely to be the cause of increasingly sophisticated and complex cyber crimes, one of which is data breaches and theft. personal data. According to Black's Law Dictionary, personal information is classified as confidential information. Please note that the information or material may be known to the named person. Thus, we can conclude that the concept of personal data protection is any means of securing data, for example via telephone. Information stored on a computer that is physically lost or visible to unauthorized persons(Rahadi, 2020).

Some countries have recognized a constitutional right to data protection, or a habeas data right, which means a person's right to trust the information they have and to correct it if errors are discovered in the information. It is clear that in this case the right to the protection of personal data is not only important, but also a key factor in human dignity and freedom. Good data protection can be a strong driver in realizing political, intellectual and religious freedom. Based on the background above, this article discusses Customer Data Protection by Bank Rakyat Indonesia in light of Law Number 27 of 2022 concerning Personal Data Protection(Nisa, 2023).

## 2. Materials and Methods

In this research the author uses normative-empirical legal research methods (applied normative law). In this normative-empirical method, the legal approach used is a statutory approach, a case approach, and a conceptual approach. The research location in this study was carried out at Bank Rakyat Indonesia (Bank BRI) Bojonegoro branch. The data sources used consist of primary legal material sources and secondary legal materials.

Where primary legal materials are data and information obtained directly from Bank Rakyat Indonesia (Bank BRI) Bojonegoro branch and secondary legal materials are data received and obtained from library materials in the form of laws and regulations related to data leaks, books and journals related to research themes. The data presentation technique in this research is presented descriptively and analytically. The data analysis technique was carried out qualitatively, and the technique for drawing conclusions was deductive.

## 3. Results and Discussion

### *3.1 Effectiveness of Customer Data Protection Against Crime (Theft of Personal Data) in the Banking Environment of Bank Rakyat Indonesia Branch Office Bojonegoro*

PT. Bank Rakyat Indonesia (BRI) is fully aware that personal information is the most important asset for its customers, therefore Bank Rakyat Indonesia really respects the confidentiality and protection of its customers' personal information in connection with the use of banking products and/or services. Customer security, comfort and privacy are Bank Rakyat Indonesia's priorities. Bank Rakyat Indonesia (BRI) implements policies and best practices in processing information related to the use of BRI banking products and/or services which are designed to protect and maintain the privacy and security of its customers' personal information in accordance with personal data protection regulations. BRI always improves its services and updates its services to protect the privacy and security of its customers' personal information.

This privacy policy regulates the policies and practices implemented by BRI in obtaining, correcting, updating, distributing, displaying, reporting, transmitting, publishing, deleting and destroying the personal information of its customers in connection with the use of personal information in accordance with Article 6 of Law Number 27 of 2022 concerning Personal Data Protection. Service products that use BRI banking products and/or services include: savings, loans and other banking services including investment products, credit cards, internet banking, Trade Finance products, BRILink services and other banking services. Websites, features, applications, social media or other communication tools provided or used by BRI. In addition, this privacy policy applies to all (registered) owners of personal data related to the use of BRI banking products and/or services.

BRI obtains and collects information that can identify and/or be identified individually or in combination with other information either directly or indirectly through electronic and/or non-electronic systems related to that information, which in this case is limited to services. Customers can provide personal information that BRI collects directly or from third parties (for example during registration or use of services, when customers contact Call BRI customer service). BRI collects customer information for various purposes, including those permitted by applicable laws and regulations in Indonesia. Personal data collected in the provision of services at BRI is general and specific in accordance with Article 4 of Law Number 27 of 2022 where general personal data as intended in paragraph (1) letter b includes: full name, gender, nationality, religion, status marriage and/or, personal data combined to identify a person.

BRI does not sell, exchange, display, publish, transfer, share and/or disclose personal information or information related to customers, visitors and users of BRI services. Customers are responsible for maintaining the confidentiality of their personal information and are responsible for the devices used for BRI services at all times. BRI is committed to protecting your personal data as best as possible as long as it is necessary to provide this service. Some customer personal information may also be managed, processed and stored by third parties who collaborate with BRI both within Indonesia and outside Indonesia to maintain service functions and fulfill effective access and supervision obligations in accordance with Article 56 of Law Number 27 of the Year 2022 con-

cerning Personal Data Protection. BRI uses two layers of security system to protect its customers' access and transactions at www.bri.co.id, namely Secure Socket Layer (SSL) and user ID and password for the ad-ministrator of the www.bri.co.id site.

From the results of field research, it is known that a number of BRI customers in Bojonegoro came to the Bri Bojonegoro branch office and reported them to ask for an explanation from the bank after the money in their savings mysteriously disappeared without any transaction. The alleged breach of BRI customer accounts was carried out through skimming (data theft) which was reported by at least five BRI customers at the Bojonegoro branch. One of them, Aris, a customer from Kota District, Bojonegoro Regency, admitted that he had never made any transactions at all, but the money in his savings account was missing amounting to IDR 12.5 million. This made him panic and he reported it to the branch for information.

Mrs. Nurmiati's customer experience, she is a customer of Bank Rakyat Indonesia Bojonegoro Branch. Mrs. Nurmiati is a 53 year old teacher. One of Ms Nurmiati's WhatsApp groups had group members sending links to wedding invitations. Links sent by group members are also broadcast messages. After Mrs. Nurmiati opened the link in the message, it felt like she was downloading an APK file. Soon after, other group members warned against visiting the invite link as it could download the APK file. This is a phishing mode with APK, where by downloading the APK file on someone's cellphone, another person can control all the cellphone data and check the contents of the account balance, as is widely reported in the news now.

Mrs. Nurmiati panicked after reading her friend's prohibition and immediately went to Bank Rakyat Indonesia customer service to discuss the problem. The customer service took action, verified Mrs. Nurmiati's account transfer which turned out to be in accordance with the previous balance, and temporarily closed the balance at Mrs. Nurmiati's request. Customer support will then help customers delete the downloaded APK file. Customer service explained that the customer's balance was safe because Mrs. Nurmiati did not use online banking on her smartphone so her account was not under the operator's control, and Customer Service was also grateful that Mrs. Nurmiati immediately informed her of that. However, because of the large number of members in the group, Nurmiati's mother was worried that her friends had downloaded the APK file link, without realizing the dangers of the APK file, and thought that it was really an invitation to her son's wedding from one of the group members. Bank Rakyat Indonesia customer service then advised the group to immediately delete the downloaded APK file and check account mutations, change the username and password to secure the account balance.

Phishing attacks targeting internet banking users are usually spread via WhatsApp. WhatsApp is a mobile application that has the same basis as Blackberry Messenger, namely a cross-platform messaging application where we can exchange messages for free. Therefore, other people who do not have access rights to other people's internet banking accounts must also understand how to avoid phishing attacks. Banking is one sector that is often exploited by phishers, and this crime not only results in the loss of customers as victims, but the banking industry also experiences a loss of trust.

In carrying out its operational activities, banking activities are always accompanied by risks. Risk in POJK Number 18/POJK.03/2016 concerning the Implementation of Risk Management for Commercial Banks is the potential for loss due to the occurrence of a certain event. According to The Office of the Comptroller of the Currency (OCC), several risk categories have been identified in the provision of internet banking services, namely: (a) credit risk; b) interest risk; (c) liquidity risk (liquidity risk); d) transaction risk; e) appeal risk (risk of compliance with requirements); f) reputation risk. The possibility of phishing is one type of operational risk. Operational Risk Based on article 1 paragraph (7) of Financial Agency Regulation Number 18/POJK.03/2016 concerning the Implementa-

tion of Risk Management in Commercial Banks, risks caused by inadequate and/or non-functioning internal processes are human activities. errors, system failures and/or external events that affect bank operations. Based on Article 53 paragraph (1) POJK Number 11/PJOK.03/2022 concerning the Implementation of Information Technology by Commercial Banks, banks are required to implement an effective internal control system in the introduction of information technology. In addition, paragraphs 1 and 2 of Law Number 19 of 15 of 2016 concerning Amendments to the Information and Electronic Transactions Law Number 19 of 2016 regulate that every electronic system owner provides a reliable and safe electronic system and is responsible for the proper functioning of the electronic system. Good. from electronic systems. Every employee of Bank Rakyat Indonesia Bojonegoro branch actively provides information security training to all customers ranging from tips to things that are safe through online banking via social media platforms such as official Twitter accounts, email messages, WhatsApp status, Instagram, YouTube, Facebook, print media. etc. The goal is to inform customers and the public about the dangers of phishing scams. This training includes: (a) Urging customers to be aware of all forms of fraud and banking crime, (b) Ignore messages from unknown and suspicious numbers, (c) The official BRI channel has been verified (green tick), (d) Do not click on links from an untrusted source, if you click on a fake link, immediately change the user, password and PIN, (e) Download application Internet banking like BRImovia Playstore/Appstore, (f) Make sure not to give personal data to anyone such as PIN, Password, OTP code, CVC/CVV code and M-token.

Bank Rakyat Indonesia Bojonegoro Branch also passively provides education to its customers, giving customers the opportunity to ask or confirm directly with the bank if they find something wrong with their savings, and customers can directly contact the Bank Rakyat Indonesia customer service office, Bojonegoro branch. The threat of cyber crime is important information for society. However, in practice, many Indonesians do not understand this, so there are still many people or organizations in Indonesia who are victims of this cyber crime. This of course must be a concern for all of us to increase public awareness of the potential for cybercrime in all our activities in the digital space. Indonesia is ranked 76th with an index value of 38.96. According to NCSI, Indonesia still gets bad scores in many subjects, one of which is education/literacy. The relationship between the above factors is very close and their fulfillment is important for effective legal protection. As the primary enforcers of electronic transactions in the banking industry, banks and the public consider their online transactions safe when bank staff themselves direct them so that online privacy can be enhanced.

With Indonesia's current condition of prioritizing online transactions compared to offline transactions, cases of fraud, especially phishing fraud, are increasing. Therefore, apart from Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016, regulations are needed that specifically regulate electronic payment transactions, especially phishing fraud. must be based on the principles that apply in the Indonesian legal system so that the effectiveness of the law in legislation can run well. Because there are still gaps in the implementation of the Information and Electronic Transactions Law in Indonesia for phishing fraud, such as: (a) People use technology freely, meaning that people are truly apathetic and do not understand the limitations of the prohibitions contained in the Information and Trade Law Electronic. (b) The thinking and skills of the Indonesian people do not yet fully understand the implications of electronic transactions. All electronic transactions are considered safe so that no illegal activity occurs. (c) Law Number 19 of 2016 concerning Amendments to the Information and Electronic Transactions Law Number 11 of 2008 does not explain the concept of phishing. Policy changes need to be made, especially Article 35 because it is close to the concept of phishing, however there are several elements of phishing that are not formulated in Article 35, giving rise to confusion in legal regulations. Law enforcement officials are not strict enough in monitoring electronic transac-

tions such as phishing scams so that they do not provide a deterrent effect, even though these crimes can disturb the public.

### *3.2 Review of the Right to Privacy in Law Number 27 of 2022 concerning Protection of Personal Data*

In fact, the increasingly massive use of internet technology and making human life easier is a substantial factor that supports an increase in the processing of personal data. It is clear that the Internet will undoubtedly become an easier means of exchanging information between individuals. Such continuous dissemination is dangerous if carried out illegally and unfair if the processing of personal data is carried out arbitrarily and in violation of applicable law. The thing you need to be careful of is that when using an internet device, all actions taken or destinations visited will be recorded and become digital traces that can be used for illegal activities. Therefore, the debate regarding abuse of personal data protection against third parties is sensitive and difficult. This problem ultimately led several countries and international institutions to develop and resolve this problem by establishing a legal framework regarding the processing of personal data. In March 2018, a case regarding personal data protection shocked the world community. There was a breach of personal data in the US via Cambridge Analytica. This was first reported by British media The Guardian.

Data analysis company Cambridge Analytica was caught using Facebook users' personal data without permission to build a system and control the US presidential election. In fact, this incident is said to be the biggest theft of personal information via Facebook in history.5

Indonesia is also not immune to personal data leaks. There have been several personal data breaches in Indonesia. For example, in April 2021, it was revealed that 533 million Facebook users had their data breached, including their full name, date of birth, gender, password, country, email address and username, which also contained the personal information of Indonesians. Apart from that, in July 2021 there was a breach in the banking sector of the data of two million BRI life insurance customers. The leak was caused by hacking of several pieces of information, such as KTP images, bank accounts, customer laboratory test reports, and customer tax information. In August 2021 there was also a flow of data: full name, date of birth, occupation, personal photo, personal identification number (NIK), passport number, Covid-19 test results, and telephone numbers of 1.3 million e-Hac application users.

The following year, in January 2022, there was another breach of Bank Indonesia data which was confirmed by the National Cyber and Crypto Agency (BSSN). As a result of this incident, 16 computers at Bank Indonesia's Bengkulu branch experienced data leaks. In the same month, there was a leak of job seeker data from PT Pertamina Training and Consulting (PTC), a subsidiary of Pertamina. The flow of information includes the applicant's full name, applicant's cell phone number, applicant's home address, place and time of birth of the applicant, applicant's diploma, transcript, BPJS card and candidate's CV. Apart from that, there was a leak of personal data. Hacker Bjorka. Bjorka hacked official government information and websites and infiltrated government officials such as Minister of Communication and Information Jhonny G Plate, Speaker of the Indonesian House of Representatives Puan Maharani, and Minister of State-Owned Enterprises Erick Thohir.

Facing the cases above, it is natural that the issue of personal data security is one of the most important aspects in the use of Internet technology, therefore a clear concept regarding privacy protection is needed as part of human rights. If we trace its history, the concept of the right to privacy was first coined by Warren and Brandheis in a Harvard University Law School research journal entitled "The Right to Privacy". In this article, Warren and Bandheis explain the idea that with technological development and progress

comes the realization that everyone has the right to enjoy life. This right is explained as the right of every person not to have their private life disturbed by other people or the state, therefore the law must be present and pay attention to the protection of privacy.

As part of human rights, in the context of implementing privacy protection which explains the recognition, respect and protection of human dignity. According to Danrivanto Budhijanno, protecting personal rights strengthens human values, improves relations between individuals and society, increases independence or autonomy in directing and achieving interests, as well as increasing tolerance and preventing discrimination and limiting government power.

The right to privacy inherent in every individual through the protection of personal data is then divided into several types, namely: (a) Data protection. This includes data privacy that applies to various personal data belonging to each individual, such as personal data, medical data, electronic mail, electronic data encryption, etc. (b) Physical privacy This includes the right to privacy, not to be suppressed, searched or detained by the government, which applies to individuals exercising the right to freedom of expression in public. (c) Privacy to find yourself. This includes privacy in determining identity, which means the freedom of each person to decide what they want without interference from other parties, such as abortion, suicide, changing religions, transgender, etc. (d) Asset privacy This includes property privacy, namely the right of every person to own identity, intellectual property and physical property.

Personal data protection is actually recognized as a type of human right and is included in international legislation. In this case, personal data protection is the meeting point between the right to information and the right to privacy through a long development process since the recognition of human rights in the Universal Declaration of Human Rights (UDHR) in 1948. common standards, namely the achievements of all nations and communities , Article 12 of the Universal Declaration of Human Rights expressly regulates the right to individual privacy, namely "No one may arbitrarily interfere in his private life, family or correspondence, or attack his honor." and reputation. Everyone has the right to legal protection against such interference or attacks.

This article also explains the concept of privacy as a general term related to the protection of other rights such as family, housing, correspondence, honor and good name. Materially it appears that the UN Convention on Human Rights offers very broad protection in relation to privacy protection. First, physical privacy, which aims to provide privacy protection regarding a person's residence. For example, although no one may enter a foreigner's home without the owner's permission, the state may not search the home without a warrant and an arrest warrant, and the state may not conduct wiretapping in the homes of its citizens. Second, decision-making privacy, which aims to provide privacy protection for someone to make decisions regarding their own life, including the life of their family. For example, a person has the right to make decisions and manage his own household without interference from other people. Third, human dignity which aims to guarantee the protection of privacy related to a person's welfare, including a person's good name and reputation. Fourth, data protection, the aim of which is to ensure privacy protection in the processing and storage of personal data.

In the Indonesian context, the state has also recognized the right to privacy as part of Human Rights as stated in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia which states that "Everyone has the right to protection of himself, his family, his honor, honor and dignity. as well as the property he controls, as well as the right to a sense of security and self-defense from fear that he will do or neglect to do something other than that. It is also explained in Article 12 of the Human Rights Convention, which means that you must not interfere in someone's personal affairs, including personal, family, household or correspondence, because everyone has the right to legal protection if a violation occurs. Article 17 of the ICCPR, which was later translated

into the decision of the Constitutional Court, explains that there must be no interference in personal, family or household affairs and every person has the right to legal protection if there is interference from other parties.

This has also been explained in the preamble to the PDP Law, that the aim of personal data protection is to guarantee the personal protection of citizens and to increase public awareness, as well as to ensure recognition and respect for the importance of personal data protection. This means that the formulation of personal data protection regulations can be understood from the need to protect the rights of individuals in society when processing personal data both electronically and non-electronically, using data processing tools. Adequate protection of personal data can give people confidence to disclose personal data in the wider public interest without abuse or violation of their personal rights. Basically, such an arrangement creates a balance between individual rights and the interests of society whose interests are represented by the state. Personal data protection rules significantly promote order and progress in society. Thus, the right to privacy of individuals in society is also indirectly included in the scope of law.

Regarding the right to privacy, it is also fulfilled in the PDP Law which is in line with the concept of human rights which are divided into two, namely deviant and non-deviant rights. According to Suparman Marzuki, rights that cannot be deviated from are absolute rights. This means that the state must not reduce enforcement even in urgent situations. Rights that cannot be deviated from include the right to life, the right to be free from torture, the right to be free from slavery, the right to be free from imprisonment for the unfortunate, the right to fulfill contracts (debts), the right to be free from retroactive punishment, the right to become subjects of law and the right to thought, belief and freedom of religion. Meanwhile, the rights are different, namely rights that can be restricted or restricted by a participating country in its implementation, such as the right to freedom of peaceful assembly, the right to freedom of association, to receive and disseminate information and ideas from all types of restrictions (whether written or verbally) and express opinions. From the previous description it can be concluded that the right to privacy is an exclusive right whose implementation can be limited or reduced in accordance with Article 15 of the PDP Law.

## 4. **Conclusion**

The effectiveness of legal protection for customers against phishing crimes in the banking environment of Bank Rakyat Indonesia, Bojonegoro branch, namely. preventive legal protection has been implemented well. However, the result of the action taken by the police is still not effective because crime is still high and the perpetrators of the crime are difficult to find because of the speed of events, banks not only close reserve accounts because they have to follow certain procedures, but also fictitious fund accounts that can be hacked. used from previous victims. identity, criminals eliminate digital traces, criminals can be everywhere, making it difficult to apply strict legal sanctions. Factors such as low knowledge about phishing crimes, facilities and infrastructure factors, community psychological factors, cultural factors regarding privacy, as well as low education and awareness factors influence the effectiveness of customer protection against phishing crimes in the banking environment, so there is a need for cybercrime threat training. From the explanation above, it can be concluded that the right to privacy is part of human rights which is specifically protected by the Personal Data Protection Law no. 27 of 2022 as a response to developments in technology, information and communication. The aim of enacting the Personal Data Protection Law Number 27 of 2022 is to protect and guarantee the basic rights of citizens in protecting the privacy of personal data. Then, the substantive framework of the Personal Data Protection Law Number 27 of 2022 is also in line with the right to privacy and the values contained in the philosophy of Indonesian society. Law Number 27 of 2022 concerning Personal Data Protection is expected to

guarantee comprehensive protection and prevent illegal activities against the personal data of Indonesian citizens.

**References**


Anggriani, A., & Arifin, R. (2019). Tindak Pidana Kesusilaan Dalam Kaitannya Dengan Kejahatan Mayantara Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik di Indonesia. *Jurnal Hukum PRIORIS*, *7*(1), 16–30.

Azwir, H. H., Wijaya, N. C., & Oemar, H. (2021). Implementasi metode single minute exchange of die untuk mengurangi waktu persiapan dan penyesuaian mold di industri polimer. *JISI: Jurnal Integrasi Sistem Industri*, *8*(2), 41–52.

Danil, E. (2021). *Korupsi: Konsep, Tindak Pidana Dan Pemberantasannya-Rajawali Pers*. PT. RajaGrafindo Persada.

Fitri, S. N. (2022). Politik Hukum Pembentukan Cyber Law Undang-Undang Informasi dan Transaksi Elektronik di Indonesia. *Jurnal Justisia: Jurnal Ilmu Hukum, Perundang-Undangan Dan Pranata Sosial*, *7*(1), 104–124.

Hariyadi, H., Misnawati, M., & Yusrizal, Y. (2023). Mewujudkan Kemandirian Belajar: Merdeka Belajar Sebagai Kunci Sukses Mahasiswa Jarak Jauh. *BADAN PENERBIT STIEPARI PRESS*, 1–215.

Haryaningsih, S., & Juniwati, J. (2021). Implementasi Program Electronic Filing (E-Filing) Dalam Upaya Peningkatan Kepatuhan Wajib Pajak Orang Pribadi Kota Pontianak Kalimantan Barat Dengan Pemahaman Menuju Era Ekonomi Digital. *Jurnal Reformasi Administrasi: Jurnal Ilmiah Untuk Mewujudkan Masyarakat Madani*, *8*(1), 32–41.

Hasan, M., & Azis, M. (2018). Pembangunan Ekonomi & Pemberdayaan Masyarakat: Strategi Pembangunan Manusia dalam Perspektif Ekonomi Lokal. CV. Nur Lina Bekerjasama dengan Pustaka Taman Ilmu.

Iskandar, I. (2020). Kapabilitas Teknologi Informasi dan Komunikasi Sekretariat Jendral DPR RI Menuju Parlemen Modern. *Inovasi*, *17*(2), 231–243.

Khansa, S. D., & Putri, K. Y. S. (2022). Pengaruh Sosial Media Tiktok Terhadap Gaya Hidup Remaja. *Ekspresi Dan Persepsi: Jurnal Ilmu Komunikasi*, *5*(1), 133–141.

Marfai, M. A. (2019). *Pengantar etika lingkungan dan Kearifan lokal*. Ugm Press.

Narew, I., & Irmawati, I. (2022). Analisis Faktor–Faktor Yang Mempengaruhi Minat Masyarakat Dalam Menggunakan Layanan E-Banking Pt Bank Rakyat Indonesia, Tbk. *JURNAL ULET (Utility, Earning and Tax)*, *6*(2), 125–144.

Ni'mah, F., Awaluddin, M., & Sijal, M. (2022). Optimalisasi Media Bisnis Online (E-commerce) dalam Mengakselerasi Penjualan Pasca Pandemi Covid-19. *Study of Scientific and Behavioral Management (SSBM)*, *3*(4), 21–28.

Nisa, R. C. (2023). Tinjauan Yuridis Tindak Pidana Terhadap Kebocoran Data Pribadi Pengguna Perdagangan Elektronik. Universitas Islam Sultan Agung Semarang.

Nursakinah, N. (2020). Upaya Peningkatan Kualitas Layanan Transaksi melalui Pemanfaatan Teknologi Informasi di Bank Sulselbar Cabang Syariah Kota Sengkang. IAIN Parepare.

Pujiono, A. (2021). Media sosial sebagai media pembelajaran bagi generasi Z. *Didache: Journal of Christian Education*, *2*(1), 1–19.

Putri, N. I., Fudsy, M. I., Karmana, D., Nasution, S. M., Munawar, Z., & Lesmana, B. (2022). Peran Akuntan Dengan Kompetensi Teknologi Informasi Pada Umkm Di Era Globalisasi. *JRAK (Jurnal Riset Akuntansi Dan Bisnis)*, *8*(2), 208–221.

Rahadi, D. R. (2020). Konsep Penelitian kualitatif plus tutorial NVivo. *PT. Filda Fikrindo, Bogor*.

Rini, R., & Harahap, P. (2021). Andorid based learning (ABL) sebagai media pembelajaran bahasa arab 4.0. LP2 IAIN Curup.

Santoso, J. (2006). *Menyiasati kota tanpa warga*. Kepustakaan Populer Gramedia.

Saputra, A. M. A., Kharisma, L. P. I., Rizal, A. A., Burhan, M. I., & Purnawati, N. W. (2023). *TEKNOLOGI INFORMASI: Peranan TI dalam berbagai bidang*. PT. Sonpedia Publishing Indonesia.

Tasyah, A., Lestari, P. A., Syofira, A., Rahmayani, C. A., Cahyani, R. D., & Tresiana, N. (2021). Inovasi Pelayanan Publik Berbasis Digital (E-Government) di Era Pandemi Covid-19. *Jurnal Ilmu Administrasi: Media Pengembangan Ilmu Dan Praktek Administrasi*, *18*(2), 212–224.

Yunita, A. R., Sari, S. P., Putri, F. E., Felissia, D. S., Fadhillana, Y. R., & Arizzal, N. Z. (2023). Hukum Perdata Nasional di Era Digital: Tantangan dan Peluang Dalam Perlindungan Data Pribadi. In *Proceeding of Conference on Law and Social Studies* (Vol. 4).