OPEN ACCESS

LAW RESEARCH

Review Quarterly

Law Research Review Quarterly is a **Journal for Law, Justice, and Crime in Indonesia and Southeast Asia**. The Journal is a peer-reviewed journal published by Faculty of Law Universitas Negeri Semarang, Indonesia. The Journal published quarterly on February, May, August, and November. ISSN 2716-3415 (Online)
Online at https://journal.unnes.ac.id/sju/index.php/snh/index

ELEGAL PROTECTION OF PERSONAL DATA AND AUTHORITY ACCOUNTABILITY FOR CYBER SECURITY: PDP LAW REVIEW

Noval bin Usman ORCID Link:
Faculty of law, Universitas Muhammadiyah Surabaya
Jl. Raya SUtorejo 59, Surabaya, East Java, Indonesia
Email : -

Satria Unggul Wicaksana Prakasa ORCID Link:
Faculty of law, Universitas Muhammadiyah Surabaya
Jl. Raya SUtorejo 59, Surabaya, East Java, Indonesia
Email : satriaunggulwp@um-surabaya.ac.id

Abstract

The problem of cyber security and personal data in Indonesia is one of the problems that cannot be underestimated. The National Cyber Security Index (NCSI) report noted that Indonesia's cybersecurity index score was 38.96 points out of 100 in 2022. This figure places Indonesia in the 3rd lowest rank among G20 countries. Globally, Indonesia ranked 83rd out of 160 countries on the report. According to Andi Fadillah Fujiama Diapoldo Silalahi , Rahmadi Islam, Singgi, and Heizkel Bram Setiawan and Fatma Ulfatun Najicha. That Cyber security is an effort to ensure the achievement and maintenance of the security nature of the organization and user assets against Legal Certainty. With this fairly limited explanation and does not cover the scope of cyber security actors, this study is here to offer the urgency of cyber security actors in being responsible and maintaining the security of a company's personal data by linking it with the PDP Law which is still relatively new. The legal issues raised in this legal research are: Responsibility of cyber security actors for leakage of personal data in a company and What is the form of legal protection in Indonesia in maintaining personal data security. The research method uses a socio-legal approach to IT and legal identification. The results of this study show that cyber security actors in a company can be held accountable in accordance with Article 30 of the PDP Law and are responsible for personal data leakage and managing personal data of users within the company. a form of legal protection for individuals in safeguarding personal data is in the form of legal products of Law Number 27 of 2022 (PDP Law).

KEYWORDS
Cyber security, Cyber crime, Data pribadi.

Introduction

The era of globalization has become very complex due to the emergence of various types of crime, many of which are related to activities on the Internet. There are at least several cases of hackers who carry out activities to subvert the government system with the intention and purpose of damaging the political stability and security of a country (Setiyawan &; Wicaksana Prakasa, 2021). Personal data protection breaches show that the cybersecurity system is still not optimal. In addition, there is also the role of a hacker in the phenomenon of cyber crime that has occurred on the site of the TNI Headquarters, the Agency for the Assessment and Application of Technology (BPPT), the National Police Headquarters and the Ministry of Foreign Affairs of the Republic of Indonesia is the other side of information technology crimes that utilize the sophistication of the internet. So are the sites of Microsoft, NASA and the Pentagon. According to Bambang Hartono's research, the incident attracted international attention. The International Information Industry Conference (IIC) Millennium 2000 held in Quebec, Canada on September 19, 2000 focused on the development of cybercrime that has the potential to disrupt technical systems and important data of companies in industrial activities. The Council of Europe's Data Protection Working Group also said that cybercrime is the worst aspect of the information society and needs to be tackled in the short term. The International Cybercrime Conference held in London in February 2001 clearly stated that cybercrime is one of the fastest-growing criminal activities on earth. The losses caused are enormous, reaching $40 billion per year. According to a study conducted by the United States Computer Security Institute (USCSI), about 90% of large companies in the United States report finding vulnerabilities in computer-based systems they use in the industrial world (Hartono, 2014).

While the application of the concept of cyber security in our country is very weak with the mark of leakage of personal data of their citizens. According to a journal by Dewi Rosadi entitled Protection of Privacy and Personal Data in the Digital Economy Era in Indonesia (2018), Explaining that privacy and personal information are the main things because, users cannot make digital transactions on a network if they feel the privacy and security of their personal information is threatened. An aspect of privacy and personal data protection relates to the way personal data, as well as sensitive user data may be processed. Disclosing personal information to irresponsible others can result in financial losses and even threaten the safety of the owner. (Dewi Rosadi &; Gumelar Pratama, 2018).

One case that is quite surprising lately is the case of leakage of 18.5 million BPJS Employment user data traded on dark forums at a price of Rp153 million. BPJS Employment Deputy for Communication Oni Marbun admitted that his party had conducted a joint investigation with the State Cyber and Encryption Agency (BSSN) and the Ministry of Communication and Information (Kominfo). From the results of the investigation, he stated that the temporary suspicion of the source of the data leak did not start from BPJS Ketenagakerjaan. The increasing cases of severe personal data loss are caused by the absence of more specific regulations to protect personal data and weak legal regulations in cyberspace or cyber aspects. This indicates that population data in Indonesia is vulnerable to misuse (HB &; Djaenab, 2022). Another case is the leak of data from the official website of the General Elections Commission (KPU) which is permanent voter list (DPT) data. The leaked data reached 204,807,203 unique data, almost the same number as the number of voters inside (DPT).

In the case of cybercrime is not limited by the universally applicable rules of international law, but we can know that the scope of cybercrime is from the means of infrastructure to commit such crimes such as through computer equipment, the internet and the target is to damage computing systems and disseminate data, obtain or even damage an internet domain with profitable and unprofitable purposes (Prakasa &; Noviandi Nur, 2019). Stating that the field of information, media, and computer analysis continues to develop without delay. Credit theft is a common crime on the rise. Hacking incidents are usually aimed at stealing certain legal materials belonging to the target. However, there are also hacks that aim to destroy certain legal documents or systems and cause digital damage and other impacts (Edrisy, 2016). Personal data refers to individuals authorized to access the data. Personal data determines who has access to that data, while data protection is a mechanism that protects data from unauthorized access. For example, a user can choose to make their profile picture visible only to contacts, everyone, or only themselves. This is called personal data. On the other hand, the data controller is solely responsible for ensuring that the user's preferences are properly met. For example, if a display image is intended to be used only by users, you should ensure that it is not unexpectedly displayed to other users (Nathaniel &; Ariana, 2021).

According to Mc Clemens that heterogeneity between individuals, economies, and public actors with respect to the acquisition, accumulation, and use of personal data. Property can be traded between all three types of actors equally. Not so with data. Individuals have less interest in obtaining data than economic actors and the public is increasingly dependent on data. The acquisition of personal data empowers economic and public actors more than just empowering individuals. Although the analogy between property and privacy allows important insight into the nature of both concepts, the difference is important enough to think that it is a mistake to treat personal data as if it were private property (McClemens, 1976).

According to Fujiama Diapoldo Silalahi, data security and data protection ensure enterprise-wide data protection This includes the human, process, and technological capabilities needed to prevent destructive forces and unwanted behavior. Data security and data protection is one of the things that must be implemented. It is mandated by more than 50 international laws and industry regulations as well as business leaders. With 2.5 trillion bytes of data generated every day and the average cost of security incidents in the big data age estimated at over $40 million, now is the time to protect sensitive personal data of customers and businesses, as well as protect other information. In other words, to take steps to keep your PII safe from internal and external threats. Data must be protected whether it resides in a production or non-production environment, in a database, application, or report. When it comes to the existence of the current PDP Law, companies clearly have an obligation to protect their personal lives. This is contained in Article 36, personal data controllers and personal data processors. The processing of Personal Data can be carried out by 2 (two) or more Personal Data Controllers with stipulated conditions (Silalahi, 2022).

Methods

This research uses socio-legal research that thoroughly examines law creation and implementation for legal policies from various scientific points of view. In the sociolegal approach, it refers to scientific disciplines and aspects of social sciences to study and apply law from various aspects with IT and legal reviews. In addition, the distinctiveness of the work of various experts in contributing to a social aspect – whether not, for example, in the field of cultural studies, social policy, or legal studies also forms the basis for understanding justifications that contribute to the diversity, dynamic and contentious understanding of social and legal matters that are also in question (Macmillan, 2008).

This research was studied with an informatics approach that studied the use of computers to organize and analyze personal data as a whole, both general and specific personal data. As well as looking at the form of legal protection and responsibility of company authorities as cyber security actors in protecting personal data, based on legal issues related to the leakage of personal data of BPJS Employment users associated with Law Number 27 of 2022 concerning Personal Data Protection.

Result and Discussion

1. Responsibility of cyber security actors for leakage of personal data in a company

A. Cyber security actors in a company

In general, an authority figure is someone who is given authority or power. What users are allowed to do is determined by the authorities. The access rights granted to a user, application, or process are referred to as authority by NIAG. The security system needs to know what rights the user has after authenticating it. Online enterprise programs, for example, must identify which accounts a user can access after using credentials to authenticate the user. The system also chooses what operations individuals are allowed to perform on their accounts, such as viewing their own transactions and balances. In the digital era, data protection is the cornerstone in maintaining human rights, therefore data protection needs to be fully guaranteed through laws and legal policy tools (Setiyawan &; Wicaksana Prakasa, 2021). The PDP Law is a new special law in Indonesia that regulates the protection of personal data. The law was promulgated on October 17, 2022 and will take effect soon. The PDP Law explains that cybersecurity involves two parties, namely the controller of personal data and the processor of personal data. Individuals, government agencies, and international organizations are examples of personal data controllers. They may act alone or jointly to identify the purpose of the personal data and administer its processing. On the other hand, individuals, government bodies, or international organizations that handle personal data on behalf of personal data controllers either alone or jointly are known as personal data controllers (hidayat fahrul, 2023).

Both have different obligations. However, in the case of leaking data of BPJS Ketenagakerjaan, which is a public legal entity. In accordance with the theory of fiction pioneered by *Freidrich Carl von Savigny*. This theory argues that legal matters that are claimed to be legal subjects are only fiction, something that individuals bring to life in their imagination to explain something, and that the subjects of law are only human beings. It is the state itself that is the creator of this legal entity. As a result, there are other subjects capable of playing a role but whose existence is not real or genuine (in this case through its representatives). Therefore, although the conditions inherent in the human body and in the law clearly do not apply to legal entities, legal entities can be considered as human beings (Suparji, 2015). So it can be concluded that the Deputy for Communication of BPJS Employment is a cyber security actor and is a controller of personal data who in his obligations is obliged to maintain confidentiality, protect, prevent and ensure the security of personal data.

B. Responsibility of cyber security actors for leakage of personal data in a company

In Article 30 Paragraph 1 of the PDP Law, if a company experiences a personal data breach, the person in charge of processing personal data must provide written notification to related parties and institutions within no later than 3 x 24 hours, if personal data protection cannot be guaranteed. Such notice shall include, at a minimum, the personal information disclosed, when and how such personal information was disclosed, and the privacy controller's efforts to handle and remediate the disclosure of such personal information. Under Article 46(1) of the PDP Law, failure to safeguard personal data refers to not taking reasonable steps to ensure its confidentiality, integrity and availability, including guarding against security weaknesses. may cause personal data transferred, stored or processed to be destroyed, lost, altered, disclosed or accessible without authorization, whether intentional or not. Meanwhile, personal data processors are not specifically regulated in the event of a data leak. However, administrative sanctions still apply in the form of written reprimands, temporary permission to process personal data, deletion or destruction of personal data, and/or administrative sanctions of a maximum of 2% of income or annual income for variable violations both personal and personal. data controllers and processors who violate established obligations (Firdaus, 2022).

C. Systematics of forming cyber security in a company

Information Security hereinafter referred to as IS is a component of cybersecurity that refers to a process and method that prevents hijacking, intrusion, use, alteration or modification in some cases of unauthorized destruction of information. Some information that is usually targeted by crime is bank account data, email, personal information, network details, profiles on social media and others (KANNO, 2005). *Application Security* is an action or security measure at the application stage with the aim of stemming data or code in the application from being stolen or hijacked. It also affects the scope of security checks present throughout application development, in this case also involving the systems and approaches taken to protect the application. The scope of application security includes hardware, software, to procedures used in identifying. A router that prevents others from seeing your computer's IP address from the Internet is a type of hardware application security However, application-level security measures are usually integrated into software, such as application firewalls, and determine exactly what activities are allowed or not allowed. The steps may include application security routines as well as include protocols such as periodic testing. (Paryati, 2008).

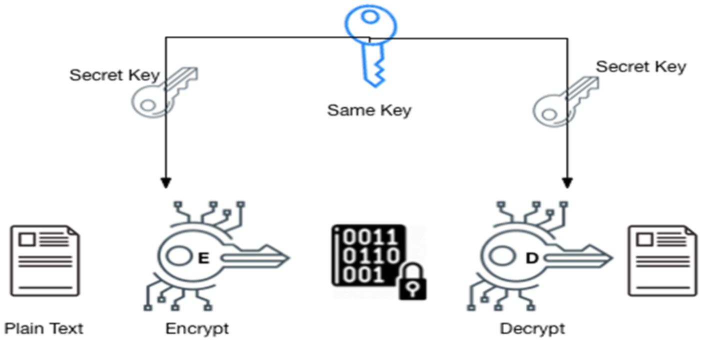
Operational Security is an element of risk management in order to protect data that is usually vulnerable to misuse, where a component will identify all important information and develop protection mechanisms to ensure its security. Network security is a security element that can prevent and protect illegal access to computer networks, so that it can configure to prevent and monitor abuse, besides that network security can also modify computer networks and resources. There are many kinds of methods that can be used to improve network security, including Email security, Web security, Wireless security, Firewall, Antivirus Software, and many other methods (Andress, 2011).

Cloud Security is an element that acts to protect various data security that has the cloud, usually the threat is in the form of piracy in service traffic, theft, and misuse of data. The implementation of this element is critical for cloud service providers to protect sensitive data from customers. Therefore, we need to meet various security requirements and procedures first, so that all forms of crime can be minimized (Ariasatya, 2021). End-User Education is the most important element in cybersecurity. This is because users or internet users lack education on cyber security so that it becomes a considerable security risk. Most of these cyber threats and crimes occur due to a lack of awareness and policy on a security system. Some gaps in cybersecurity can occur through text messages, downloading applications, use on social media, using email, and creating and using passwords (Roscoe et al., 2017).

D. The role of corporate authorities in implementing personal data security

Encryption Algorithm has a relationship with Cryptography which is an application in the field of advanced mathematics that aims to protect information or data stored and sent in a certain format to the system or person who has the right to read and process the data. Indirectly Encryption is at the heart of cryptography. Encryption itself is the process of converting messages into a format that cannot be read by eavesdroppers or eavesdroppers. One form of explanation of the encryption algorithm is the process of changing the character of information from plain text to unreadable text (cipher text) (Rahardjo, 2017). Encryption algorithms are divided into 2 categories, namely, symmetric encryption of asymmetric funds:

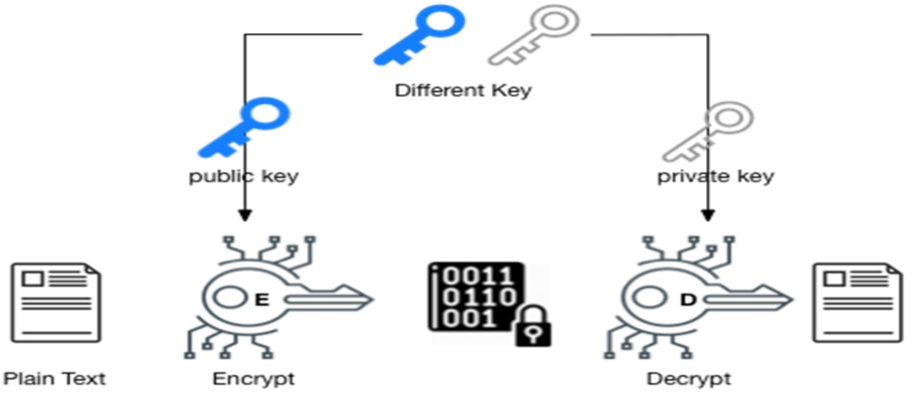
Symmetrical Enscription:



Picture 1.1 Systematic display of symmetric encryption algorithm
Source: https://socs.binus.ac.id/

Symmetric encryption encrypts plaintext and decrypts encoded text with the same single phrase. One of the earliest and most effective encryption methods was symmetric encryption. The keywords used can be words, numbers, or random strings of characters. In a computer network, the password used for data exchange will be the same for both the sender and receiver. Symmetric encryption techniques include Caesar, Blowfish, and AES, for example. This kind of encryption has the disadvantage that the message conveyed can be decrypted by other parties if using the same password.

Asymmetric Encryption:

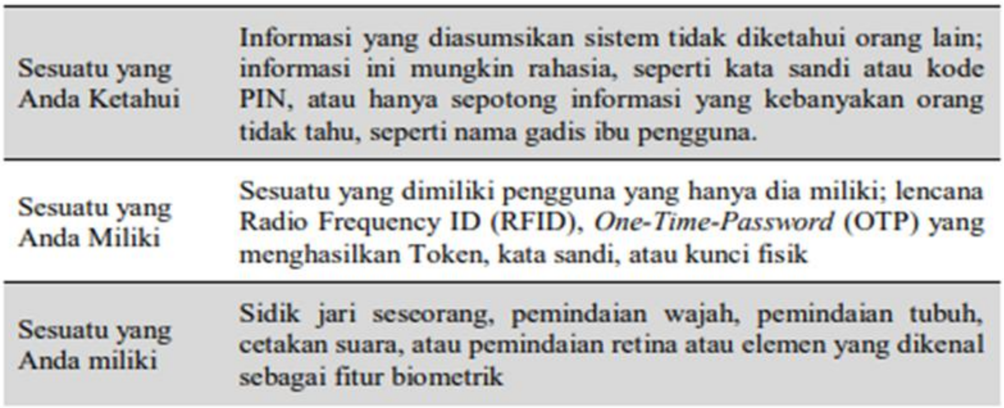


Picture 1.2 Systematic display of Asymmetric Encryption Algorithm
Source: https://socs.binus.ac.id/

Asymmetric encryption encrypts data between the encryption and decryption stages using two different passwords. Comparing this encryption to symmetry, it's fairly new. The term "decryption" refers to the process of decrypting data; The term "public key" is used to encrypt data. A public and private key pair is generated. Both the sender and receiver store the private key in a file in their own settings or programs. We refer to this type of encryption as end-to-end encryption. RSA is an example of a frequently used algorithm (Salim et al., 2020).

Authentication is essential for any security system, because it is the key to verifying the source of a message or that someone is who he claims to be. NIAG defines authentication as a security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authority to receive certain categories of information.

Table 1.3 Some important aspects for security authentication

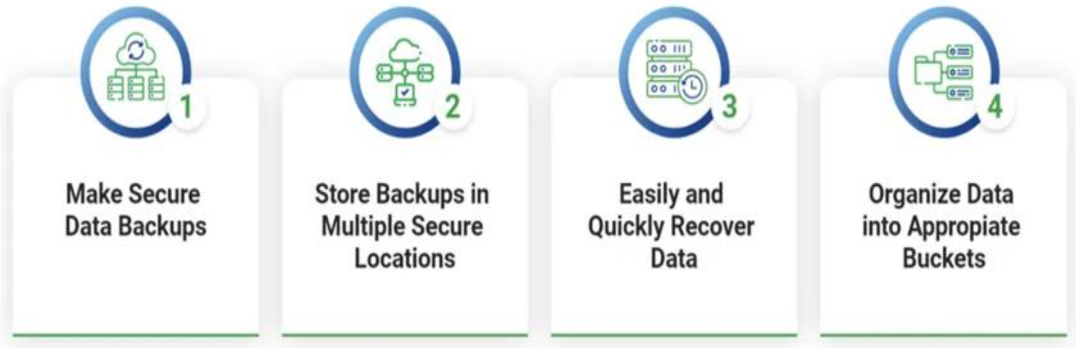


Sesuatu yang Anda Ketahui	Informasi yang diasumsikan sistem tidak diketahui orang lain; informasi ini mungkin rahasia, seperti kata sandi atau kode PIN, atau hanya sepotong informasi yang kebanyakan orang tidak tahu, seperti nama gadis ibu pengguna.
Sesuatu yang Anda Miliki	Sesuatu yang dimiliki pengguna yang hanya dia miliki; lencana Radio Frequency ID (RFID), *One-Time-Password* (OTP) yang menghasilkan Token, kata sandi, atau kunci fisik
Sesuatu yang Anda miliki	Sidik jari seseorang, pemindaian wajah, pemindaian tubuh, cetakan suara, atau pemindaian retina atau elemen yang dikenal sebagai fitur biometrik

Source:https://eprints.amikom.ac.id/id/eprint/18330/1/Dasar%20Cyber%20Security.pdf

If an authentication system requires more than one of these factors, the security community classifies them as systems that require multi-factor authentication. Two examples of the same factor, such as a password combined with a user's mother's maiden name, are not multifactor authentication, but combine fingerprint scanning and *a Personal Identification Number* (PIN) because it validates something that the user owns that fingerprint and something that the PIN user knows. In almost all services that require the highest security such as enterprises require multiple layers of authentication. This will be done in the field of companies such as diversion of funds, theft of deposits, taking customer funds will not occur (Rahmadi Islam, 2018). Companies implement multiple layers of authentication such as using a password to sign in to apps, but some require scanning. face, retinal scan, finger print and others. Authentication also plays a role in validating the source of a message, such as a network packet or email. At a low level, message authentication systems cannot rely on the same factors applicable to human authentication. Cryptographic signatures are often relied upon in message authentication systems, which consist of the digest or hash of the message generated with the secret key. The recipient can verify the sender of the communication because only one person has access to the key that creates the signature. It is hard to believe that a person is who he says he is or that a communication comes from the person he claims to be without a voice authentication mechanism (Hanafi, 2022).

By utilizing data, there are various benefits that companies can get. For example, streamlining business processes, increasing revenue, to help solve problems and make decisions. But when companies depend on data, the higher the obligation to protect the data. That's why the term data resilience or data resilience is an important topic today. If defined, data resilience is the ability of data infrastructure to always be available and accessible even if the company experiences disruptions, problems, or unwanted disasters (Cervone, 2007). Top-tier colocation data centers are designed to meet compliance standards and maintain data resilience and business continuity in the event of disasters, power outages, cyberattacks, and equipment failures. Physical buildings are built to withstand the physical impact of natural disasters, while internal infrastructure has measures to maintain operational time and protect assets (Kusumaputri et al., 2018).


1
Make Secure Data Backups
2
Store Backups in Multiple Secure Locations
3
Easily and Quickly Recover Data
4
Organize Data into Appropiate Buckets

Picture 1.5 Data durability principles
Source: https://www.tierpoint.com/

First things first: make sure you back up each data set as a whole safely, regularly, and successfully. After all, there's nothing more disappointing than finding that your files lost data after you used the latest backup to restore them. Keep in mind: there are solutions, such as backup as a service (BaaS), on the market that can automate the backup and restore process for you. They are designed to save time and ensure your data is available and backups are maintained for all workloads in your organization's cloud and on-premises environments. Having data redundancy is necessary, otherwise you risk a single point of failure. Consider creating physical and digital backups that are securely stored in multiple cloud locations and physical vaults so that if one location is compromised during an unexpected disruption, such as a cyberattack, you can still access data from other secure locations (Aji, 2023).

Also, when storing backups offsite, make sure they are properly encrypted and your IT team has a smooth process of handling encryption keys. If your organization needs help securing its sensitive data, cloud providers can provide encrypted, geolocation, and redundant storage to enhance security. An important part of a data resilience strategy is having the ability to recover your data easily. It's important for your recovery process to meet your organization's recovery time goals and recovery point goals; and your IT team should be able to recover everything from a single deleted file to a complete data set after a ransomware attack or business interruption. When designing your strategy, data segmentation should be a major concern. As you group data, you can then easily identify and prioritize which data sets need to be recovered first in case of an outage. After all, a server that handles payments or fulfills payroll is a bigger priority than a chat server (Kusnadi, 2021).

One of the three acceptable methods of achieving data sanitization is a software-based process that securely overwrites digitally stored information with random binary data according to certain standards, then verifies and certifies that the deletion has been successful. Secure data deletion can occur in both active and idle environments across a variety of IT assets, such as servers, PCs/laptops, mobile devices, removable media, and removable drives, as well as in virtualized data centers and large cloud environments. For digital storage devices, erasing data means zeros and ones will be overwritten definitively across device sectors. This makes all data permanently unrecoverable while maintaining the functionality of the device. For targeted sanitization, data deletion means that a specific file, folder, or location, such as a LUN, [1]is overwritten verifiably and leaves the untargeted area intact and operational (Hughes & Coughlin, 2006).

Actual elimination is critical so that companies in the public and private sectors can guard against data vulnerabilities, comply with various data protection regulations, use resources efficiently, and implement green practices all in a complex portfolio of IT assets. File delete commands generally don't actually delete data; They simply remove the clues to the disk sector where the data is located. Such "deleted" data can be easily recovered with common software. However, proper data sanitization is critical for data and device lifecycle management, such as device rollback and data migration. Because companies typically use a wide array of drive and device technologies, it's important to apply the right methods to the right equipment to get the right results, including when performing remote

[1] A logical unit number (LUN) is a unique identifier that designates individual hard disk devices or devices grouped for addresses by protocols associated with SCSI, iSCSI, Fibre Channel (FC) or similar interfaces. A LUN is a central management of block storage arrays shared over a storage area network (SAN).

wipes, when data storage assets are located very far from technicians. Erasing data allows organizations to verify that their data cannot be recovered and provides organizations with tamper-resistant deletion certificates to ensure compliance with a growing number of data protection regulations, including regulations that have data minimization, the "right to erasure," or the "right to erasure requirements." It also helps organizations transition towards more sustainable circular business models and move away from less environmentally friendly methods of destroying data and devices. With data wipe, organizations can safely resell or reuse devices without having to worry about sensitive data being compromised, while significantly reducing e-waste (Rupp et al., 2022).

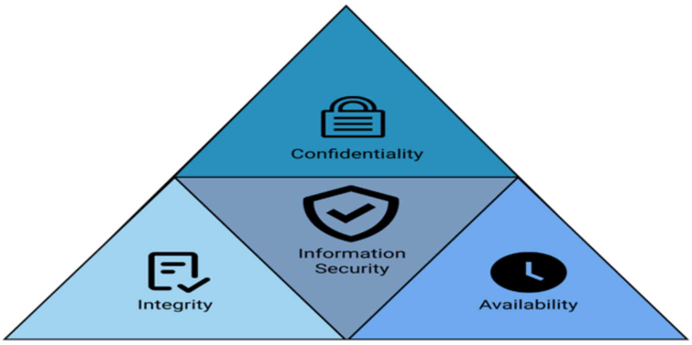
Basically data masking is the process of hiding data by changing the original letters or numbers. Regulatory and data protection requirements require businesses to protect the sensitive data they collect about their customers and operations. Data masking creates fake versions of an organization's data by altering sensitive information. Various techniques are used to create realistic and structurally similar changes. Once the data is closed, the original data values cannot be reverse-engineered or tracked without accessing the original data set. On the other hand, Data Masking masks sensitive or confidential application data so that it can be safely replicated to nonproduction systems. Using sophisticated prebuilt or customized concealment techniques, IT organizations can maintain the characteristics of genuine information and maintain data and referential integrity. Realistic yet unidentified data improves the quality of test data, which, in turn, improves the quality of development, testing, and training. Data privacy solutions can be easily tailored to each organization's business needs, further improving quality and accelerating adoption. Businesses need applications to function and these applications require maintenance and testing, new applications are developed as the company grows (Ravikumar, 2011).

Access control is an important component of security because it limits who has access to certain information, programs, and resources. Digital venues are secured with access control regulations, just as physical locations are secured with pre-approved locks and guest lists. This policy, inadvertently, keeps the wrong people away and allows the right people in. Technologies such as authorization and authentication are also required for the operation of access control rules. By doing this, companies can clearly ensure that users are the users they claim to be and that their access levels match their device, role, and context (Asrianda, 2016). \

Access controls to sensitive information, such as customer data and intellectual property obtained through fraud by hackers and other unscrupulous users, are maintained. Access control reduces the risk of employee data loss and also prevents data loss on web-based platforms. As an alternative to manually entering information, most organizations will likely provide identity management and access control solutions to improve access control. How access control works In its simplest form, Access Control provides user identification based on their fingerprint and gives them the appropriate access threshold when they log in. Security tokens, such as PINs, passwords, and biometric fingerprints, are typically used as a kind of collateral to identify and authenticate users. Multi-factor authentication (MFA) improves external data security by requiring users to verify using several different methods. Once the user's identity is verified, access control measures are provided (Penelova, 2021).

E. Application of CIA concepts and data protection management in ensuring the confidentiality of personal data

The CIA Triad can be defined as a design model used to guide an individual or persons within a particular organization in the design or creation of applications, systems, procedures, or policies pertaining to information security support. The CIA's own triad consists of confidentiality, integrity, and availability. These three aspects are considered the most important aspects in building strong and effective information security. (Harahap et al., 2023).



Picture 1.5 CIA Triad Consep
Source: https://student-activity.binus.ac.id/csc

These three terms are considered the three most important concepts in information security. As explained in each letter that represents the basic principles of cybersecurity. Considering these three principles can also be a guide for developing an organization's security policy. CIA Triad helps companies focus on finding vulnerabilities based on confidentiality, integrity, and availability features when evaluating needs and use cases for new products and technologies. The CIA triad is very useful in security situations and situations, especially when each component is critical and sensitive. However, it is also useful when developing systems that require data classification and the management of permissions and access rights. Companies must also strictly implement the CIA triad when addressing vulnerabilities in an organization's network. This can be an effective tool to prevent the chain of cyberkillings, which is the process of targeting and executing cyberattacks (Amrozi et al., 2021).

The CIA Triad helps you identify what crackers might target and properly implement policies and tools to properly protect those assets. In addition, the CIA Triad can be used to train employees on cybersecurity. Use what-if scenarios and real-world case studies to help employees make policy decisions about the confidentiality, integrity, and availability of information and systems. Effective information security management also includes comprehensive processes and practices to address common information security risks. Examples include the development and implementation of information security policies, identity and access management, network and systems security management, and information security training for employees and other stakeholders. When managing information security within an organization, the CIA helps companies identify and manage information security risks more effectively. By maintaining the confidentiality, integrity, and availability of information, businesses can reduce information security risks and protect critical assets from security threats (Vansuri et al., 2023).

2. Legal protection in Indonesia in implementing personal data security

A. Policy of Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection

The PDP Law itself is a manifestation of Article 28G paragraph (1) of the 1945 Constitution. Which states "Everyone has the right to personal, family, honor, nobility and property guarantees. under his influence, and having the privilege of feeling that everything is fine with the world and a guarantee from the danger of fear to do or not achieve something that is common freedom". One form of alignment in this case is contained in the words "personal guarantee" and "guarantee from danger" which indirectly say that all kinds of things related to the person of an individual absolutely receive legal protection, including personal data (Soraja, 2021). Based on Article 1 Paragraph 2 of the Data Protection Law, personal data protection refers to the overall efforts of personal data protection at the time of processing personal data in order to guarantee the constitutional rights of personal data subjects. In the PDP Law there are personal data controllers and personal data processors. A personal data controller is any Individual, public authority and international organization acting individually or jointly to determine the purposes of personal data and control the processing of personal data. The subject of personal data is nothing but the individual to whom such personal data relates, that is, us as a society. The rights of personal data subjects are further regulated in Articles 5 to d. Article 15 of the PDP Law includes, among others, the right to obtain information regarding the identity, legal basis, purpose of request and use of personal data and the applicant's responsibility for such personal data, the right to stop processing, deletion and/or destruction of personal data. protection of personal data concerning him, and the right to sue him and obtain compensation for violations of personal data processing. (Sudayono, 2023).

However, based on Article 15 paragraph (1) of the PDP Law, it states that the rights of Personal Data Subjects as referred to in Article 8, Article 9, Article 10 paragraph (1), Article 11, and Article 13 paragraph (1) and paragraph (2) are excluded for: (national defense and security interests; the interests of law enforcement processes; public interest in the framework of state administration; the interests of supervision of the financial services sector, monetary, payment system, and financial system stability carried out in the framework of state administration; interest of statistics and scientific research). What is meant by Interest in the law enforcement process is understood as needs related to efforts or procedures for implementing or enforcing laws and regulations based on its provisions, such as the process of investigation, investigation, prosecution, and so on. Then what is meant by public interest in the context of state administration, such as population control, social security, taxation, customs, and business licensing services that are integrated electronically. While what is meant by personal data processor is Individuals, public authorities, and international organizations that individually or jointly process personal data on behalf of the controller. The obligations of the personal data controller are regulated in Articles 20 to d. Article 50 of the Data Protection Act provides for the obligation to provide evidence of consent given by the data subject to the processing of personal data, the obligation to maintain the confidentiality of personal data, and the obligation to prevent unauthorized access to personal data. On the contrary, the obligations of personal data processors are stipulated in Articles 51 to d. Article 52 of the PDP Law regulates the obligation to process personal data at the request of the personal data controller and the obligation to obtain written permission from the personal data controller before entering into a contract with another personal data processor (Fauzi &; Radika Shandy, 2022).

In general, criminal justice is carried out based on the Criminal Procedure Law, which is a procedural law that contains rules regarding the process of solving or handling criminal cases, including investigation, investigation, prosecution, trial, Investigation Process, Appeal, Cassation, and Judicial Review. The Criminal Procedure Code and the Criminal Code itself are lex generali in criminal law. That is, if in addition to the Criminal Procedure Code and the Penal Code there are other laws that regulate special procedural law and certain criminal sanctions, then these provisions are considered special provisions. However, in the PDP Law itself, criminal sanctions are regulated for the following acts: (Any person who intentionally and unlawfully obtains or collects personal data that does not belong to him with the intention to benefit himself or others which may result in the loss of the personal data subject shall be sentenced to imprisonment for a maximum of 5 years and/or a maximum fine of Rp5 billion. (Article 67 paragraph (1) of the PDP Law). Any person who intentionally and unlawfully discloses personal data that does not belong to him shall be sentenced to imprisonment for a maximum of 4 years\ and/or a maximum fine of Rp4 billion. (Article 67 paragraph (2) of the PDP Law). Any person who intentionally and unlawfully uses personal data that does not belong to him shall be sentenced to imprisonment for a maximum of 5 years and/or a maximum fine of Rp5 billion. (Article 67 paragraph (3) of the PDP Law). Any person who intentionally creates false personal data or falsifies personal data with the intention to benefit themselves or others which may cause harm to others shall be sentenced to imprisonment for a maximum of 6 years and/or a maximum fine of Rp6 billion. (Article 68 of the PDP Law)). Based on the provisions above, the crime of identity theft as you ask can be charged using Article 67 paragraphs (1) and (3) of the PDP Law, namely with a maximum prison sentence of 5 years and/or a maximum fine of IDR 5 billion. In addition, victims can file a civil lawsuit based on Article 26 paragraphs (1) and (2) of Law Number 19 of 2016 (ITE Law) if the relevant provisions: (Unless otherwise stipulated by legal regulations, the use of information regarding a person's personal data through electronic media requires the consent of the data subject. Any person whose rights are violated under subsection (1) may bring a claim for damages incurred under this Law). Claims for compensation against parties who misuse personal data are in the form of lawsuits against the law based on Article 1365 of the Civil Code (Pane et al., 2023).

B. Protection of personal data security within the company

Prior to a personal data leak, the controller and data processor may take preventive measures as a measure to protect personal data. On the other hand, companies can also find loopholes and minimize fraud or check the administrative field in a company. Other deliveries that can be done are; due diligence, digital audit and maintenacne system. In the application of due diligence must first take a risk-based approach to cyber due diligence in transactions. Cyber due diligence is not yet established and does not analyze standardized data like other types of due diligence in general. Since all transactions are not the same, they do not require the same level of diligence. Companies should have processes in place to evaluate the current threat landscape and identify external and internal criminals who may be targeting parties to transactions (Maharani Wulan, 2011). These conditions can vary by industry or region, and higher-risk transactions such as country-specific acquisitions or in sectors that have recently experienced an attack require greater precision. The more active a business is in conducting transactions like a company. More and more cyberspace must be woven into the transaction lifecycle in general. Frequent acquirers must establish relationships with cybersecurity stakeholders in their companies and have flexible cyber transaction guidelines in place to help handle cyber at every stage of the transaction, level of cyber risk, and type of transaction. This enables these companies to use cybersecurity at key points in the deal lifecycle and manage cyber risk to their existing targets and portfolios more effectively. Another outcome of managing cyber risk in transactions is to establish cyber readiness benchmarks, which can be applied to other businesses in its portfolio and used when assessing new investments. Some will conduct annual security assessments of their portfolio companies, to further prepare them for future deals (Coco & De Souza Dias, 2021).

Cybersecurity audits aim to assess compliance and identify vulnerabilities and other problem areas across the digital infrastructure. Audits not only help organizations stay ahead of cybercriminals, they also help avoid fines. On-site audits include auditors, usually third-party vendors, who check your software configuration; they may also run tests to analyze your network and identify any gaps. Network security audits are great at highlighting potential solutions to strengthen your security practices, controls and risk mitigation. In short, having a second view may be the difference between being protected and being the victim of the next cyberattack (Jadhav, 2023).

System maintenance refers to the process of proactively monitoring, managing, and updating hardware, software, applications, and systems on a device or network to ensure they function optimally and pose no threat to system security or performance. System maintenance is critical because threats to system security or performance are constantly evolving, and system maintenance provides a proactive way to counter these threats (Ignatius Deradjad Pranowo, 2019). The importance of system maintenance in cybersecurity cannot be overstated. Cyberattacks are on the rise, and hackers are getting bolder and more sophisticated in their tactics. These attackers typically use a combination of different attack vectors, including malware, phishing, exploitation of software vulnerabilities, and more, so proactive maintenance of critical systems is necessary. System maintenance can be divided into two broad categories: proactive and reactive. Proactive system maintenance focuses on preventing security breaches before they happen. This approach involves regular backups, software updates, vulnerability scanning, and setting security alerts to ensure that modifications to the system are closely monitored, and early signs of impending breaches are clearly visible to system administrators. In contrast, reactive maintenance targets errors or security breaches that pass or occur despite many precautions having been implemented initially (Amadi-Echendu et al., 2015).

There is currently no separate court for cyber law enforcement settlements. In general, parties representing the business world or other business actors usually choose out-of-court settlement through alternative dispute resolution (ADR) or arbitration, which is often an option. This is because the decision is final and binding. Not only that, but choices can also be made quickly, by experts, and behind closed doors. to maintain a favorable business environment. In addition, arbitral awards have the same executive authority as judicial awards. Arbitration has complete competence in accordance with Law Number 30 of 1999 concerning Arbitration and Alternative Dispute Resolution. The parties should have reached an agreement on the PDP lawsuit (STISNU Nusantara, 2016). Since each party is free to choose arbitrators, PDP arbitration also provides the parties with access to settlement options. The parties must sign an arbitration agreement at the beginning of their marriage or add an arbitration clause in their contract to use arbitration. In reality, the arbitration rules accepted by the arbitral tribunal always allow the parties to make an initial non-judgmental settlement also referred to as negotiation, mediation, or arbitration (ADR) before entering into arbitration. Unlike the place of arbitration where the outcome is up to you, alternative dispute resolution (ADR) decisions are mutually beneficial. In reality, ADR awards are passed as arbitral awards in accordance with the techniques and models of Mediation Arbitration (Wahyuningdiah, 2018).

Conclusion

Indonesia already has several policies governing cyber security as well as personal data. One of them is the PDP Law, but it is still relatively less taboo. Especially with the implementation of cybersecurity that is still ineffective marked by frequent cyber leaks that involve the threat of people's personal data. Therefore, the government needs to take the implementation of cyber security seriously. Besides instead of preparing legal preventive policies as a backup plane if a data leak has occurred. With the existence of legal products that are binding on cybersecurity actors and the security of individual personal data. This includes the responsibilities of cybersecurity actors in the corporate or institutional sector in the event of a data leak and also policy policies that protect their personal data. Cybersecurity systematics that must be applied in every company can be a good standard as a first step in implementing strong cyber security. In addition, there are individuals or groups who try to violate norms and laws, violate rules and regulations, or take control of information security and physical assets whether material or non-material benefits. Therefore, the government needs to make some serious efforts to anticipate cyber threats and attacks and save Indonesia's cyber defense from being targeted by irresponsible parties.

References

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah*

Politik Dalam Negeri Dan Hubungan Internasional, *13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Amadi-Echendu, J., Hoohlo, C., & Mathew, J. (2015). Cyver physical system in future maintenance. *Lecture Notes in Control and Information Sciences*, *20*(February), v–vi. https://doi.org/10.1007/978-3-319-15536-4

Amrozi, Y., Nadiya, K., & Rahmah, L. (2021). *TANTANGAN SECURITY DN KEHANDALAN SISTEM DALAM APLIKASI BERGERAK*. *4*, 1–10.

Andress, J. (2011). Operations Security. *The Basics of Information Security*, *June*, 81–95. https://doi.org/10.1016/b978-1-59749-653-7.00006-2

Ariasatya, A. R. (2021). Cloud Security : Blockchain Access Control. *I-Finance*, *2*(1), 1–15.

Asrianda. (2016). *Pengaturan Kontrol Akses bagi Pendataan Data*.

Cervone, H. F. (2007). Computer Network Security and Cyber Ethics (review). In *portal: Libraries and the Academy* (Vol. 7, Issue 2). https://doi.org/10.1353/pla.2007.0017

Coco, A., & De Souza Dias, T. (2021). "Cyber Due Diligence": A patchwork of protective obligations in international law. In *European Journal of International Law* (Vol. 32, Issue 3). https://doi.org/10.1093/ejil/chab056

Dewi Rosadi, S., & Gumelar Pratama, G. (2018). Urgensi Perlindungandata Privasidalam Era Ekonomi Digital Di Indonesia. *Veritas et Justitia*, *4*(1), 88–110. https://doi.org/10.25123/vej.2916

Edrisy, I. F. (2016). PENGANTAR HUKUM SIBER. In *Jurnal Penelitian Pendidikan Guru Sekolah Dasar* (Vol. 6, Issue August).

Fadillah, A. (2021). EKSISTENSI KEAMANAN SIBER TERHADAP TINDAKAN CYBERSTALKING DALAM SISTEM PERTANGGUNGJAWABAN PIDANA CYBERCRIME. *Eksistensi Keamanan Cyber*, *6*(4).

Fauzi, E., & Radika Shandy, N. A. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Jurnal Lex Renaissance*, *7*(3), 445–461. https://doi.org/10.20885/jlr.vol7.iss3.art1

Firdaus, M. A. (2022). Ruang Lingkup Perlindungan Data Pribadi: kajian Hukum Positif Indonesia. *Ganesha Law Review*, *4*(1), 13–17.

Hanafi. (2022). Dasar cyber security dan forensic. *Dasar Cyber Security Dan Forensic*.

Harahap, A. H., Difa Andani, C., Christie, A., Nurhaliza, D., & Fauzi, A. (2023). Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder. *Jurnal Manajemen Dan Pemasaran Digital*, *1*(2), 73–83.

Hartono, B. (2014). Hacker Dalam Perspektif Hukum Indonesia. *Masalah-Masalah Hukum*, *43*(1), 23–30.

HB, B., & Djaenab. (2022). Tinjauan Yuridis Perlindungan Data Pribadi Terkait Kebocoran Data Dalam Ruang Cyber Crime Artikel. *Petitum*, *10*(1), 70–76. https://uit.e-journal.id/JPetitum

hidayat fahrul, D. (2023). *KAJIAN HUKUM PERLINDUNGAN DATA*

PRIBADI DALAM PERATURAN PERUNGAN-UNDANGAN INDONESIA.

Hughes, G., & Coughlin, T. (2006). Tutorial on Disk Drive Data Sanitization Data Loss is Rampant. *Nist Special Publication*, *Volume|*, 1–15. http://tomcoughlin.com/Techpapers/DataSanitizeTutorial121206b.pdf

Ignatius Deradjad Pranowo. (2019). *Sistem dan manajemen pemeliharaan*.

Jadhav, krishna D. (2023). *The Role of Cyber Security Audits in Managing Company Systems and*. *April*, 0–7.

KANNO, Y. (2005). An introduction to information security evaluation. *Journal of Information Processing and Management*, *48*(6), 320–332. https://doi.org/10.1241/johokanri.48.320

Kusnadi, S. A. (2021). Perlindungan Hukum Data Pribadi Sebagai Hak Privasi. *AL WASATH Jurnal Ilmu Hukum*, *2*(1), 9–16. https://doi.org/10.47776/alwasath.v2i1.127

Kusumaputri, P., Prihatin, B., & Riyanti, D. (2018). Hubungan Resilience At Work Dengan Kinerja Marketing Officer Di Pt X. *Jurnal Ilmiah Psikologi MANASA*, *7*(2), 110–120.

Macmillan, P. (2008). *EXPLORING THE "SOCIO" OF SOCIO LEGAL STUDIES*. 282.

Maharani Wulan. (2011). *Analisis Penerapan Customer Due Diligence (Prinsip Mengenal Nasabah) Dalam Transaksi Ekspor-Impor Dengan Letter of Credit Pada PT. Bank X*. 1–146.

McClemens, J. H. (1976). Privacy and the individual. *Nat.Hosp.Hlth Care*, *1*(12), 7–10.

Nathaniel, E., & Ariana, I. G. P. (2021). Data Pribadi Pengguna Layanan Jejaring Layanan. *Data Pribadi Pengguna Layanan Jejaring Layanan*, *9*(7).

Pane, V., Tampongangoy, G., & Koloay, R. N. (2023). Perlindungan Hukum Terhadap Data Pribadi Konsumen yangn Diretas berdasarkan Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik. *Lex Privatum*, *9*(2), 1–10.

Paryati. (2008). Keamanan Sistem Informasi. In *Seminar Nasional Informatika 2008 (semnasIF 2008) UPN "Veteran" Yogyakarta, 24 Mei 2008* (Vol. 2008, Issue semnasIF).

Penelova, M. (2021). Access Control Models. *Cybernetics and Information Technologies*, *21*(4), 77–104. https://doi.org/10.2478/cait-2021-0044

Prakasa, S. U. W., & Noviandi Nur, P. E. (2019). Analysist of cyber espionage in international law and indonesian law. *Humanities and Social Sciences Reviews*, *7*(3), 38–44. https://doi.org/10.18510/hssr.2019.736

Rahardjo, B. (2017). *Keamanan Informasi & Jaringan*. 47. http://budi.rahardjo.id/files/keamanan.pdf

Rahmadi Islam. (2018). PENGATURAN TINDAK PIDANA MAYANTARA (CYBER CRIME) DALAM SISTEM HUKUM INDONESIA. *PENGATURAN TINDAK PIDANA MAYANTARA (CYBER CRIME) DALAM SISTEM HUKUM INDONESIA*, □□□□□ □□□□(3), 1–13.

http://dx.doi.org/10.1186/s13662-017-1121-6%0Ahttps://doi.org/10.1007/s41980-018-0101-2%0Ahttps://doi.org/10.1016/j.cnsns.2018.04.019%0Ahttps://doi.org/10.1016/j.cam.2017.10.014%0Ahttp://dx.doi.org/10.1016/j.apm.2011.07.041%0Ahttp://arxiv.org/abs/1502.020

Ravikumar, justus rabi. (2011). Design of Data Masking Architecture and Analysis of Data Masking Techniques for Testing. *Article in International Journal of Engineering Science and Technology*, *7*(January 2015), 177. https://www.researchgate.net/publication/230639917

Roscoe, R. D., Craig, S. D., & Douglas, I. (2017). End-user considerations in educational technology design. *End-User Considerations in Educational Technology Design*, *June*, 1–400. https://doi.org/10.4018/978-1-5225-2639-1

Rupp, E., Syrmoudis, E., & Grossklags, J. (2022). Leave No Data Behind – Empirical Insights into Data Erasure from Online Services. *Proceedings on Privacy Enhancing Technologies*, *2022*(3), 437–455. https://doi.org/10.56553/popets-2022-0080

Salim, A., Putra Gyantana, P., Pengadaan Sapras, S., & Pendidikan Kabupaten OKU Selatan, D. (2020). Seminar Hasil Penelitian Vokasi (SEMHAVOK) ANALISIS PERBANDINGAN KRIPTOGRAFI ALGORITMA DES, BLOWFISH, MD5 DAN CHIPER UNTUK KEAMANAN DATA. *Seminar Hasil Penelitian Vokasi (SEMHAVOK)*, *3*(2), 180–184.

Setiawan, H. B., & Najicha, F. U. (2022). Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data. *Jurnal Kewarganegaraan*, *6*(1), 976–982.

Setiyawan, R., & Wicaksana Prakasa, S. U. (2021). Indonesian Online Shopping Practices in the COVID-19 Pandemic Era: A Study of Culture and Cyber Security Law. *Jurnal Hukum Novelty*, *12*(01), 29. https://doi.org/10.26555/novelty.v12i01.a16944

Silalahi, F. D. (2022). Keamanan Cyber (Cyber Security). *Penerbit Yayasan Prima Agus Teknik*, 1–285. http://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/367

Singgi, I. G. A. S. K., Suryawan, I. G. B., & Sugiartha, I. N. G. (2020). Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime). *Jurnal Konstruksi Hukum*, *1*(2), 334–339. https://doi.org/10.22225/jkh.2.1.2553.334-339

Soraja, A. (2021). Perlindungan Hukum Atas Hak Privasi dan Data Pribadi dalam Prespektif HAM. *Prosiding Seminar Nasional Kota Ramah Hak Asasi Manusia*, 20–32.

STISNU Nusantara. (2016). *Modul Matakuliah Arbitrase penyelesaian Sengketa* (Vol. 4, Issue 1).

Sudayono, G. wahyu dawani; (2023). *KEBIJAKAN HUKUM PIDANA DALAM UU PDP*. 1–13.

Suparji. (2015). TRANSFORMASI BADAN HUKUM DI INDONESIA oleh SUPARJI. In *Repository.Uai.Ac.Id*. www.uai.ac.id

Vansuri, R., Fauzi, A., Prasetyo, E. T., Negara, R., & ... (2023). Peran CIA (Confidentiality, Integrity, Availability) Terhadap Manajemen Keamanan Informasi. *Jurnal Ilmu ...*, *2*(1), 106–113. https://www.greenpub.org/JIM/article/view/234%0Ahttps://www.greenpub.org/JIM/article/download/234/206

Wahyuningdiah, K. (2018). *Kingkin Hukum Alternatif Penyelesaian Sengketa dan Arbitrase.pdf*.

***

DECLARATION OF CONFLICTING INTERESTS

The author declares that there is no potential conflict of interest in the research, authorship, and/or publication of this article.

FUNDING INFORMATION

None

ACKNOWLEDGMENT

None

HISTORY OF ARTICLE

Submitted : January 10, 2023
Revised : January 17, 2024
Accepted : February 12, 2024
Published : February 26, 2024