JMI Jurnal Multidisiplin Indonesia

Volume 4 Number 11, 2025
E-ISSN: 2964-9048 | P-ISSN: 2963-2900
https://jmi.rivierapublishing.id/index.php/rp

Legal Protection of Personal Data in Relation to the Use of Cloud Computing in Indonesia

Gomulia Oscar, Bernadete Nurmawati, Adi Darmawansyah
Universitas Bung Karno, Indonesia
Email: goscarvb@yahoo.com

Abstract

Rapid developments in information technology have encouraged the use of cloud computing as a solution for data storage and processing, including personal data. However, despite its benefits, cloud computing systems carry serious risks of data leaks and misuse. This study examines legal protection regulations for personal data in the context of cloud computing use in Indonesia and analyzes implementation challenges. The research employs a normative juridical method with a regulatory approach and secondary legal materials. Results indicate that Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) provides a comprehensive framework, regulating data subjects' rights, controllers' and processors' obligations, and cross-border transfers. Implementation faces challenges, including delays in establishing a supervisory authority, absent implementing regulations, low digital legal literacy, and unprepared cloud-based providers. To enhance effectiveness, steps are needed such as creating an independent authority, enacting regulations, boosting literacy, and fostering international cooperation. Legal challenges arise from inadequate derivative regulations, non-functional supervision, and weak infrastructure and awareness among businesses. Solutions include accelerating supervisory agency formation, drafting detailed regulations, and elevating stakeholder literacy and compliance.

Keywords : *Legal Protection; Personal Data; Cloud Computing*

Corresponding Author; Gomulia Oscar
E-mail: goscarvb@yahoo.com

INTRODUCTION

The era of globalization has changed the role of information technology to a very strategic position because it can bring about a world without boundaries, distance, space, and time, as well as increase productivity and efficiency (Alcácer, Cantwell, & Piscitello, 2016). The shift in social and cultural order, economic life, and the development of law are the results of technological developments (Volti & Croissant, 2024). Almost all aspects of people's lives are directly connected to technology and bring benefits to development (Galperin & Fernanda Viecens, 2017). The convenience created by the development of computers provides many benefits for users (Bansah & Darko Agyei, 2022). The continuous development of the internet means that a person's personal information can be easily accessed by others (Baybarin, Afonin, Maksimenko, Goncharov, & Singilevich, 2020). In the current development of information technology, various activities in the context of government, business transactions, commerce, and communication take place through electronic media (*online)* (Schnoll, 2015). Information technology includes systems that *collect*, *store*, process, produce, and send information to and from industries or communities

effectively and quickly (Yamin, 2019).

The world of information technology has created a number of situations that humans had never thought of before (Brown & Duguid, 2017). Such rapid technological developments, especially in the world of computing, have made it much easier for humans to do their work (Sciences et al., 2017). Progress has always been made in tandem between software and hardware (Patterson & Hennessy, 2016).

One of the developments in information technology is a revolution in computer technology that can store large amounts of data, known as *cloud computing*, which is a combination of computer technology ('computing') and internet-based development ('cloud'). *Cloud computing* is a technology that uses the internet and remote central servers to maintain or manage customer data (Groom, 2018). *Cloud computing* helps consumers and businesses to use applications without installation, accessing their personal files anywhere using internet access (Attaran & Woods, 2019). This technology enables efficiency by centralizing data storage, processing, and memory (Lee, Kim, Ko, & Yoo, 2024). In addition, another advantage of *cloud computing* is that it can increase customer business productivity so that customers no longer need to invest and spend money to build data centers (Attaran, 2017). Furthermore, *cloud computing* can be utilized quickly and easily and has very high mobility because it can be accessed via the internet (Stergiou & Psannis, 2017).

Cloud *computing* can be defined as large-scale devices or computers that are online (not necessarily using the same hardware) and use networks and servers to manage data (Moura & Hutchison, 2016). The infrastructure and software provided by cloud computing are supplied by service providers (Banditwattanawong, Masdisornchote, & Uthayopas, 2016). These service providers have set up remote networks with online systems. Examples of *cloud computing* in everyday life include *web-based* email such as Yahoo and Microsoft Hotmail, photo storage such as Google Picassa, and social networking such as Facebook. Meanwhile, the major international players in cloud computing are Google, Yahoo, Microsoft, Amazon, and Oracle (Kiswani, Dascalu, & Harris Jr, 2021).

Cloud computing is a combination of computer and internet usage, which is currently a new industry but is showing sharp growth as users utilize the services *of cloud computing* providers to store data, including customer privacy data (Sunyaev, 2020). The use of *cloud computing* has many benefits. In addition to reducing operational costs because customers only pay for the services they use, customers also do not need to provide infrastructure and software when using *cloud computing* applications, because all of that is provided remotely by the provider using the internet. In addition, due to its highly mobile nature *(based on the internet)*, customers can access it anytime and anywhere, making it more efficient (Kamilaris & Pitsillides, 2016).

While offering benefits, the use of *cloud computing* also raises new legal issues, namely the violation of customer privacy, as the data storage activities offered by *cloud computing* include data related to customer activities (*account activity)*, making the

identity of each customer who accesses the system and other important information highly susceptible to misuse, resulting in the violation of personal data privacy. This is especially true if users store their data in programs hosted on other people's hardware, as they will lose control over their highly sensitive personal information. In this situation, the responsibility to protect this information from irresponsible parties (such as hackers) and internal data breaches lies with the *cloud computing* provider. There are concerns when personal data containing highly important *(*sensitive) information falls into the hands of other parties or companies. In other words, there is a fundamental concern that the use *of cloud computing* has the potential to increase the risk of personal data breaches if there are no clear rules.

Cloud computing offers various advantages, but it also has security risks that must be managed properly. Therefore, organizations and individuals using *cloud* services need to implement **proactive security strategies,** including data encryption, multi-factor authentication, and regular monitoring and auditing to reduce the risk of data leaks or loss.

Cloud computing systems are one of the things related to personal data that must be protected. One case is the data breach experienced by Yahoo, which announced that 1 billion of their user accounts had been hacked by unknown parties in August 2013, which was only reported in September 2016. The stolen account information included, among other things, user names, email addresses, phone numbers, dates of birth, randomized passwords, and in some cases, encrypted or unencrypted security questions and answers.

From this case, there is an interest in providing personal data protection equivalent to that of other countries. There is the potential for crimes to occur that originate from searching for someone's personal data, the removal of identity data of criminals from *search engines* (e.g., google.com and bing.com). Considering all of the above threats and potential violations, the personal data protection regulation is intended to protect the interests of personal data and provide economic benefits for Indonesia.

According to Jerry Kang, personal data describes information closely related to an individual that distinguishes their characteristics. Basically, the form of data protection is divided into two categories, namely the form of data protection in the form of security for physical data, both visible and invisible data. Another form of data protection is the existence of regulations governing the use of data by unauthorized persons, misuse of data for certain interests, and destruction of the data itself.

The legal protection of personal data in the use *of cloud computing* is regulated by Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection (PDP Law). The protection of personal data in the use of *cloud computing* aims to maintain the confidentiality of user data and prevent data misuse. In this case, it is essential and crucial for personal data to be kept confidential. Problems with personal data will arise when the confidentiality of personal data cannot be protected, making it vulnerable to misuse by unauthorized parties. Since the enactment of the

PDP Law, personal data managers are required to obtain permission or consent from data owners to manage their personal data and also before transferring personal data to other parties outside the jurisdiction of Indonesia.

The objectives of this research are essential in ensuring that regulatory and doctrinal analysis effectively resolve emerging personal data risks in cloud computing ecosystems; therefore, this study aims to (1) analyze Indonesia's statutory personal data protection framework in relation to the use of cloud computing, and (2) examine the persistent legal challenges limiting supervisory authority, regulatory harmonization, infrastructure enforceability, and provider compliance in personal data governance for cloud computing services in Indonesia, while also delivering both theoretical and practical benefits. Theoretically, this research contributes to the development, enrichment, and systematization of the literature on civil law-based personal data protection, data sovereignty principles, cross-border computing jurisdiction, and identity-authenticated access governance in cloud environments, reinforcing statutory clarity for academic references, legal doctrine, and regulatory benchmarking, and practically, the research is expected to (a) improve awareness and compliance guidance for cloud users, including individuals, businesses, and cloud tenants sharing public or private cloud infrastructure, (b) provide enforceability baselines and best-practice recommendations for local and foreign cloud providers operating multi-jurisdictional servers involving Indonesian data subjects, and (c) evaluate gaps in government oversight related to supervisory authority delays, derivative regulation absence, security audit mechanisms, encryption enforcement, incident reporting standards, and documented access isolation in cloud computing, ultimately strengthening policy direction for integrated national compliance and recovery mechanisms for personal data breach victims and stakeholders.

RESEARCH METHOD

This study employed normative legal research (doctrinal research), which prioritized statutory interpretation, legal doctrine, conceptual analysis, and secondary legal materials. It treated law as a binding norm and analytical tool for evaluating regulatory implementation, drawing from Seorjono Soekanto's view that such research encompassed analytical-descriptive and prescriptive approaches to assess regulatory certainty and enforceability.

Secondary legal data were sourced from regulatory frameworks, judicial literature, case documentation, academic doctrine, journals, books, and archives. These included primary materials (e.g., Law Number 27 of 2022 concerning Personal Data Protection, or PDP Law), secondary materials (peer-reviewed journals and articles), and tertiary sources (legal dictionaries and digital regulations).

Data collection involved library research through structured review and synthesis of documented materials, focusing on statutory substance, comparative principles, doctrinal arguments, and governance concepts related to personal data protection in cloud computing.

Data analysis used statutory and doctrinal interpretation with descriptive-

normative synthesis to address research problems, enhance argument clarity, and support regulatory conclusions logically.

RESULTS AND DISCUSSION

Regulations on Legal Protection of Personal Data in Relation to the Use of Cloud Computing in Indonesia

The widespread development of technology and information has made personal privacy a threat because it can be accessed by irresponsible people. Personal data protection in Indonesia does exist, but it does not provide clear certainty and does not provide protection for the community. The regulations in Indonesia are scattered across various regulations, and these regulations do not provide detailed explanations. Many articles that protect personal data are still general in nature and do not provide comprehensive protection for personal data. In addition to the lack of comprehensive protection, there is also the weakness of the absence of laws that provide guarantees of recovery for victims whose privacy or personal data rights have been violated. There are no regulations specifically aimed at this issue in Indonesia, but there are several regulations that have been enacted, although they are not specific:

1. **Law No. 36 of 1999 on Telecommunications**

   According to the Government Regulation of Year 2000 on Telecommunications Implementation, an implementing regulation of Law No. 36 of 1999 concerning Telecommunications, the internet is formally classified as a multimedia-based telecommunications service that delivers information through network infrastructure, placing it under the legal domain of telecommunications law. The Indonesian Criminal Code has not yet provided explicit jurisdictional and procedural regulation for cybercrime, which affects the completeness of privacy and personal data protection because modern technology enables unauthorized data access without the knowledge or consent of the data owner. Although ministerial regulations are legally incorporated within the telecommunications regulatory regime, Law No. 36 of 1999 implicitly reinforces information confidentiality obligations, where Article 22 prohibits any unauthorized, unlawful, manipulative, or deceptive access to (a) telecommunications networks, (b) telecommunications services, and (c) specific or special-purpose telecommunication networks, while Article 40 forbids interception or wiretapping of any information transmitted across telecommunications infrastructure, thereby obligating service providers to maintain user data confidentiality, and positioning violations as legally admissible offenses subject to criminal sanctions, fines, evidentiary recording, and procedural legal proceedings under Indonesian law.

1. **Law No. 19 of 2016 concerning Electronic Information and Transactions (ITE Law)**

   The absence of comprehensive regulations on personal data protection makes the ITE Law a reference for understanding the legal basis of personal

data protection. The Indonesian Criminal Code does not yet regulate cybercrime, which has implications for personal rights. In the cyber world, the issue of protecting an individual's personal rights is closely related to the protection of data subjects. This is because technological developments are advancing, making it possible for other parties to access an individual's data without the data owner's knowledge. Therefore, it is very likely that an individual's personal rights will be violated. Legal action under the ITE Law is only in the form of civil lawsuits. Article 9 explains that the use of information technology must protect personal data. Business actors who offer services or products through electronic systems must provide complete and accurate information regarding the terms of the contract, the manufacturer, and the products offered.

Article 26 paragraph (1) of the ITE Law normatively affirms that personal data contained in information distributed via electronic media may only be processed, published, or transmitted based on the explicit consent of the data owner, positioning personal data protection as an inseparable component of constitutional privacy rights and personal autonomy. This statutory provision reflects three core dimensions of privacy rights: (a) the right to enjoy private life free from interference, (b) the right to communicate without surveillance or interception, and (c) the right to exercise full control over access to personal information and identity-linked data. Under this article, Electronic System Operators (ESOs) are legally bound to guarantee confidentiality, deploy appropriate security safeguards, and are strictly prohibited from disclosing or disseminating stored personal data without lawful authority. However, Article 26 does not yet embed secondary norms providing direct criminal sanctions for personal data privacy violations, meaning that legal remedies for misuse or unauthorized data disclosure remain limited to civil litigation as governed by Article 39 paragraph (1), which refers to lawsuits filed under applicable procedural law, while the substantive punitive mechanism for intentional unlawful acts against electronic documents—alteration, deletion, transfer, concealment, or system-enabled dissemination—is regulated separately under Article 32 paragraph (1), which mandates a maximum imprisonment term of 8 years and fines of up to 2 billion rupiah. When such violations are committed by corporations and involve systematized misuse or large-scale dissemination of personal data, legal accountability and evidentiary procedure may rely on Supreme Court Regulation No. 13 of 2016 on the handling of corporate criminal cases to strengthen the enforcement pathway, even though a dedicated supervisory authority for personal data governance mandated by the PDP Law remains critical for closing regulatory and enforcement gaps in cross-jurisdictional cloud computing environments.

The ITE Law comprehensively contains provisions on how data is provided to individuals, legal entities, and the government. The ITE Law strictly

prohibits unlawful access or acts that are against the law by using electronic systems to obtain personal data by breaking through security systems. The ITE Law explicitly states that wiretapping is a strictly prohibited act, except for parties with legal authority, such as those with legal interests. Based on the ITE Law, it is stated that everyone is prohibited from disclosing personal data to the public in any way. Furthermore, data protection will not only regulate access but also opening and changing, such as manipulating, altering, deleting, or destroying data so that it appears to be authentic.

Regarding acts related to unauthorized access to data or *unlawful access*, the ITE Law states that "any action that can cause electronic systems to be disrupted in a systematic manner ( ) that prevents data owners from accessing their personal data is prohibited." Protection under this law is not only for data security, but also means securing the electronic systems where the data is stored. Protecting electronic systems also means protecting **the** data **itself.**

2. **Ministry of Communication and Information Technology Regulation No. 20 of 2016 concerning Personal Data Protection in Electronic Systems**

The Minister of Communication and Information Technology Regulation governing personal data protection (Perkominfo No. 20/2016 and its second amendment, Permenkominfo No. 21/2017) obligates every Electronic System Operator (ESO) to guarantee confidentiality, safeguard data owner information, and strictly restrict personal data usage solely for the purposes declared at the point of lawful collection, with all processing, utilization, and dissemination requiring explicit consent from the data owner, while Article 15 mandates that all stored personal data must be encrypted to ensure system-level data isolation, controlled access, and document security. These regulations provide multi-process protection covering data acquisition, collection, processing, analysis, storage, display, announcement, transmission, dissemination, access governance, and data destruction, as well as defining data subject rights, user obligations, and ESO compliance duties; however, the regulatory regime remains limited to administrative sanctions—verbal warnings, written warnings, temporary operational suspension, and public violation notices published through official network sites—for any unauthorized, unlawful obtainment or system-enabled misuse, and it does not yet specify an exhaustive legal definition of personal data, creating derivative regulatory gaps that weaken binding authority. Because the supervisory authority mandated under the PDP Law is not yet operational and sanctioning mechanisms remain administrative rather than punitive, many ESOs and foreign-based cloud-linked providers have not yet aligned internal governance with compliance duties such as encryption baselines, incident reporting, deletion protocols, authenticated isolation access, and documented audit logs, as administrative penalties alone are perceived to lack coercive power, even though the regulations allow a two-year compliance adjustment period and provide formal dispute and ministerial complaint

channels, making infrastructure strengthening and OPDP operationalization critically necessary for enforceability amid cross-jurisdictional cloud ecosystems.

3. **Government Regulation No. 71 of 2019 on Electronic System and Transaction Operators (PP PSTE)**

The regulatory expansion for personal data protection introduced under Government Regulation No. 71 of 2019 (PP PSTE) is considered insufficient in meeting Indonesia's long-term national protection requirements, as although new safeguards have been incorporated, they remain temporary in nature, lack comprehensive punitive deterrence, and hierarchically hold a lower legal position than statutory law, limiting their enforceability when stronger legal authority is required. The regulation's development has also created implementation frictions across industry and society, particularly in the interpretation of data governance duties and compliance expectations. Moreover, the absence of direct criminal sanctions for personal data violation cases under this derivative regulation reduces its coercive and corrective power despite representing progress in Indonesia's digital legal transformation.

In the initial and unrevised PP PSTE formulation, the government mandated service owners and cloud computing providers to place servers within Indonesia, primarily to stimulate domestic investment growth in national data center infrastructure and create economic incentives for local technological stakeholders. However, international cloud service providers expressed skepticism toward local data center ecosystems, citing concerns that Indonesian data residency carries increased vulnerability to misuse due to historically weak, fragmented protection frameworks and infrastructure governance gaps. Following the regulatory revision, service providers were granted conditional flexibility, allowing electronic systems and non-strategic personal data to be stored and processed outside Indonesia under specific governance and jurisdictional conditions.

As a regulatory compromise, the Indonesian government introduced formal segmentation of data into three categories: strategic, high-risk, and low-risk, where strategic personal data—such as national identification numbers, family cards, and intelligence agency records—must remain stored within Indonesia due to sovereignty and national security implications, while high-risk and low-risk classifications may be stored abroad, though still requiring provider-supervised access control and documented account governance, particularly within private system infrastructures. Despite this stratification, challenges persist where cloud providers operating across jurisdictions may evade domestic enforceability arguments by seeking refuge under foreign regulatory frameworks, potentially reducing Indonesian legal accountability and hindering electronic evidentiary jurisdiction when enforcement involves cross-border cloud ecosystems.

Indonesia's digital transformation needs continue to grow proportionally

with its population scale, prompting urgency for a more integrative statutory framework that ensures end-to-end personal data protection enforceability beyond administrative penalties alone, considering that emerging threats such as hacking, phishing, malware, unauthorized corporate disclosure, cloud multi-tenancy leakage, and insider exploitation create amplified risk in ungoverned cross-platform infrastructures. While the ITE Law affirms broad jurisdiction, applying domestic sanctions even for foreign perpetrators targeting electronic systems located within Indonesia (Article 2 & 27), enforcement capability remains contingent on identifiable violations carrying direct legal consequences in Indonesia and actionable complaint pathways for impact-based prosecution. However, comprehensive cloud-specific protection still requires OPDP operationalization, infrastructure governance strengthening, regulatory derivatives clarity, encryption baselines enforcement, incident reporting standardization, access isolation, and auditable legal accountability across stakeholders—as highlighted by the current legal ecosystem limitations.

4. ***International Covenant on Civil and Political Rights*** **(ICCPR) through Law Number 12 of 2005**

   Indonesia has strengthened its commitment to human rights protection by ratifying the International Covenant on Civil and Political Rights (ICCPR) through Law No. 12 of 2005, which legally incorporates the Covenant into the national regulatory system with binding force while complementing other previously ratified international instruments, thereby obligating the state to harmonize domestic legal frameworks and policies with global standards for civil and political rights guarantees, including personal privacy and autonomy protection. As a core treaty within the International Bill of Human Rights, the ICCPR mandates member states to respect and ensure fundamental rights such as the right to life, freedom of religion, expression, and assembly, and the right to a fair trial, while Article 16 explicitly affirms universal legal recognition of individuals as legal persons before the law, and Article 17 establishes robust protection against arbitrary or unlawful interference with privacy, family, home, correspondence, communications, and dignity, guaranteeing that every individual has the right to legal safeguards and protection from unauthorized surveillance, data misuse, or reputational attacks. The implementation of ICCPR obligations is periodically monitored and evaluated by the UN Human Rights Committee through mandatory state-submitted accountability reports and compliance reviews, where the Committee assesses alignment between national regulations and Covenant standards and issues corrective recommendations as part of a global oversight mechanism that reinforces state accountability, legal enforceability benchmarks, and rights recovery direction for affected data subjects and stakeholders within dynamic cross-border digital infrastructures, including cloud computing environments where personal data governance depends on regulatory clarity, jurisdictional enforceability, and

institutional compliance supervision.

Legal Challenges in the Implementation of Personal Data Protection in Cloud Computing Services in Indonesia

The development of information technology, particularly the use of cloud computing, has brought about major changes in the management and storage of personal data. Cloud computing allows data to be stored virtually via the internet, both within and outside the jurisdiction of Indonesia. This situation poses new challenges in the legal protection of personal data, as follows:

5. Regulatory Weaknesses

The PDP Law also regulates cross-border data transfer. Articles 56 and 57 of the PDP Law state that personal data may only be transferred abroad if the destination country has an equivalent or higher level of data protection, or if there is an international agreement, or with the consent of the data subject. This provision is highly relevant to the cloud computing model, which generally involves servers in various countries.

Although Indonesia already has the PDP Law, in practice there are still a number of legal and technical challenges in its application to cloud computing services, including:

a. Uncertainty Regarding Data Storage Location (Data Sovereignty Issue)
   Cloud computing allows personal data to be stored on servers across multiple countries, raising issues of legal jurisdiction. Indonesia faces difficulties in ensuring that the data of its citizens stored abroad remains protected in accordance with national standards.
b. Lack of Compliance by Foreign Cloud Providers
   Many foreign-based cloud service providers are not necessarily subject to Indonesian law.
c. Indonesia or do not yet have internal systems that are in line with the PDP Law, including in terms of incident reporting, data deletion, and access restrictions.
d. Lack of Supervision and Law Enforcement
   The absence of an effective personal data protection supervisory authority has resulted in weak oversight of data processing in cloud computing. In addition, investigations into violations occurring outside Indonesia's jurisdiction are very limited.
e. Unpreparedness of Businesses and Users
   Many businesses, especially MSMEs and startups, do not yet fully understand their obligations as data controllers, nor how to choose cloud service providers that comply with personal data regulations. Public awareness of their rights as data owners is also still low.

Based on the above legal challenges, a comprehensive approach is needed in terms of regulation, institutions, and education:

a. Establishment of a Personal Data Protection Authority (OPDP)

The PDP Law mandates the establishment of an independent supervisory agency. This agency must be established immediately and given sufficient authority to supervise, investigate, and impose sanctions for data violations, including in the context of cloud services.

b. Strengthening of PDP Law Derivative Regulations

The government needs to immediately enact implementing regulations that elaborate on the provisions of the PDP Law, particularly regarding:

1) Technical and security standards for cloud computing,
2) Criteria for cross-border data transfers,
3) Audit guidelines for cloud providers.

c. International Cooperation

To address cross-border issues, Indonesia needs to establish international or bilateral cooperation on personal data protection and adopt global principles such as the OECD Privacy Guidelines or the General Data Protection Regulation (GDPR) as minimum standards.

d. Improving Digital Legal Literacy

Educating the public and business actors is key to ensuring that data protection is implemented from upstream to downstream. The government and the private sector can hold training sessions, socialization events, and public campaigns related to personal data rights and digital security.

6. Lack of User Awareness.

Many internet users are not yet aware of the importance of protecting their personal data. This ignorance is often caused by a lack of adequate education on privacy and data security issues. Most users do not understand how their personal data can be misused or exploited by irresponsible parties. For example, many are unaware that the information they share on social media can be used to steal identities or commit fraud.

The lack of understanding about the risks of personal data leaks is also exacerbated by the complexity of the technology used. Many users find it difficult to keep up with developments in security technology and good data protection practices. They often neglect basic security measures such as using strong passwords, regularly updating software, or enabling two-factor authentication. In addition, users also tend not to read the privacy policies or terms and conditions applied by online applications and services, so they are unaware of how their data is collected, stored, and used. This lack of awareness also creates loopholes that can be exploited by cybercriminals. Without sufficient knowledge on how to protect personal data, users become easy targets for various forms of cyberattacks such as phishing, malware, and ransomware. Therefore, it is crucial to increase user awareness and understanding through effective education programs and public campaigns. With better knowledge, users can take proactive measures to protect their personal data and reduce the risk of data misuse in the digital world.

7. Threats from Cybercrime

Cybercrime such as hacking, phishing, and malware continues to grow and pose a serious threat to personal data security. Cybercriminals are becoming increasingly sophisticated in exploiting system vulnerabilities to steal personal data. One crime that harms cyber users due to the ease of accessing information is the theft of personal information. Personal information can include personal data, ATM data, and credit card data. They use various sophisticated techniques to deceive users and breach security systems, often with the aim of gaining financial profit or sensitive information. Phishing, for example, involves deception designed to trick individuals into revealing their personal information by posing as a trusted entity. Hacking and malware attacks can damage systems, steal data, or even encrypt user data to demand a ransom.

In addition to traditional methods such as phishing and malware, cybercriminals are also beginning to leverage new technologies to carry out attacks. Artificial intelligence (AI) and machine learning-based attacks enable criminals to carry out more targeted and difficult-to-detect attacks. Deepfake technology, which enables the creation of highly convincing fake videos or audio, can also be used for malicious purposes, such as fraud or identity theft. Increasingly complex Distributed Denial of Service (DDoS) attacks can paralyze online services and disrupt business operations, creating additional vulnerabilities to personal data leaks. Furthermore, cybercrime attacks often target weaknesses in the technological infrastructure of companies and organizations. Outdated systems, poor security configurations, and reliance on old technology provide loopholes for cybercriminals to exploit.

According to the Organization of European Community Development (OECD), cybercrime is any form of illegal access to data. Any unauthorized action using a computer, particularly to access, transmit, or manipulate data, constitutes cybercrime. Some examples of cybercrime cases in Indonesia include the theft of personal data due to data leaks.

Small and medium-sized companies are often the main targets because they may not have the resources or expertise to implement strong security measures. Even large companies with sophisticated cybersecurity teams can fall victim to cyberattacks if they are not careful and vigilant against evolving threats.

The inability of individuals and organizations to effectively deal with cybercrime threats can result in significant financial losses, damage to reputation, and loss of customer trust. In addition, personal data breaches can have long-term consequences for affected individuals, including the risk of identity theft and financial fraud. Therefore, it is essential to raise awareness and capabilities in identifying and countering cybercrime threats, as well as adopting a layered security approach that includes advanced technology, user training, and strong security policies.

8. Legal Challenges in the Implementation of Cyber Notaries

The implementation of cyber notaries in Indonesia is a step forward in modernizing notary services. However, the legal challenges faced in its implementation are quite complex. One of the main challenges is the issue of legal recognition of electronic signatures. According to the ITE Law, electronic signatures have the same legal force as wet signatures. However, in practice, there are still doubts among the public and legal practitioners regarding the validity and authenticity of these electronic signatures. Furthermore, another challenge is the protection of personal data. With the existence of cyber notaries, important data and documents will be stored digitally, thereby increasing the risk of data leaks. The newly passed PDP Law regulates how personal data must be managed and protected. However, the implementation and supervision of compliance with this law is still a big task for the government and related institutions. Another legal aspect that needs to be considered is the existence of clear and strict regulations regarding cyber notaries. Currently, there are no specific provisions that regulate cyber notaries in detail. This has led to legal uncertainty, where digital notary practices can be high risk for the parties involved.

Therefore, it is important for the government to immediately formulate regulations governing cyber notaries in order to provide legal certainty and protect all parties involved. In addition, technical challenges cannot be ignored. Adequate and secure technological infrastructure is essential to support the implementation of cyber notaries. Issues such as uneven internet access and cybersecurity are major concerns. The adoption of technology by notaries also requires training and a good understanding of digital devices. Without strong technical support, the implementation of cyber notaries will face significant obstacles. Finally, public trust in cyber notaries is an equally important challenge. The public needs to be convinced that digital notary services are safe and reliable. Education and outreach on the benefits and security of using cyber notaries must be carried out intensively. Only by increasing public trust can the implementation of cyber notaries run smoothly and provide optimal benefits to society. As technology evolves, these challenges must be addressed with an adaptive and innovative legal approach.

9. The Challenge of Isolation and Multi-Tenancy

As organizations increasingly expand their services and data digitally, the need for comprehensive identity and access management is becoming more urgent. This need is particularly important in multi-tenant environments, where user data isolation and the protection of sensitive information across multiple clients are critical to avoid potential breaches of confidentiality and integrity. In this context, ensuring properly segmented access controls and strict monitoring mechanisms are in place is essential to prevent unauthorized access and maintain compliance with regulatory standards, as the implications of a data breach can extend beyond the affected organization

and impact all tenants within it. In a public cloud environment, where multiple organizations share the same infrastructure, there are concerns about inadequate data isolation between tenants. This risk can lead to data leaks between organizations using the same cloud services.

10.Insider Threat Challenges

Internal threats are one of the main challenges in identity and access management. These internal threats can manifest in various ways, including employee negligence, malicious intent, or misuse of access rights, posing significant risks to an organization's information assets and overall security posture. Addressing these risks requires a multifaceted approach that includes not only robust technological solutions but also an effective governance framework and continuous monitoring to detect and mitigate potential insider threats before they can cause harm. Furthermore, organizations must recognize that relying solely on technological measures is not sufficient; they must also foster a culture of security awareness and accountability among employees, as this can significantly reduce the likelihood of insider threats stemming from negligence or poor judgment. Furthermore, implementing comprehensive employee training programs that educate staff about the potential implications of their actions and instill a sense of accountability can serve as a preventive measure against increasing insider threats, ultimately improving the organization's resilience to such risks.

11.Compliance and Regulatory Challenges

As more companies expand their online delivery of services and data, they must ensure that only authorized individuals can access sensitive information and resources. This is reinforced by increasing regulatory scrutiny and the need for transparent access management processes that not only comply with existing laws but also anticipate future needs in a rapidly changing legal landscape. This is underscored by increasing regulatory scrutiny and the need for transparent access management processes that not only comply with existing laws but also anticipate future requirements in a rapidly changing legal landscape, as organizations must grapple with the complexity of personal data protection laws in various jurisdictions. As these regulations evolve, organizations must implement comprehensive strategies that encompass data protection and ethical considerations, ultimately aiming to foster trust and security in their identity management systems while mitigating risks associated with data breaches and unauthorized access to personal information.

12.Identity and Access Management (IAM) Challenges

Identity and access management has become an increasingly important field in the modern information technology environment.The emergence of complex internal structures in large organizations, coupled with the need for small and medium-sized businesses to ensure security without the burden of expensive infrastructure, drives the need for effective practices in information

technology service management to maintain high service quality. This is important as organizations strive to remain competitive while protecting their information assets and ensuring service continuity amid evolving security challenges. Additionally, increasing user expectations for improved service quality and simultaneous pressure from regulatory bodies for documented access control processes highlight the urgent need for organizations to enhance their identity management systems to effectively balance security, cost, and compliance requirements. Furthermore, integrating identity governance with privileged access management presents a promising approach for organizations to strengthen their security framework, enabling them to manage and control access to sensitive data more effectively while simplifying processes. Furthermore, organizations must also recognize that traditional identity verification methods are inadequate in the digital landscape, requiring the implementation of more sophisticated and standardized identity management practices that not only enhance security but also facilitate collaboration across platforms and jurisdictions.

As organizations increasingly expand their services online, the implementation of robust identity management practices becomes crucial in safeguarding sensitive information and maintaining user trust, compounded by the challenge of ensuring that only authorized individuals have access to critical data and resources. To address these challenges, a comprehensive identity and access management framework must be developed, one that not only encompasses technological solutions but also the policies and processes necessary to adapt to the dynamic nature of the organizational environment and user expectations. Furthermore, the evolution of identity management requires a thorough exploration of the limitations inherent in the current model, as well as the development of innovative approaches that can adapt to the diverse environments and use cases that exist in today's digital landscape, ultimately driving the creation of more secure and efficient systems.

CONCLUSION

The use of cloud computing for storing and processing personal data in Indonesia posed complex legal challenges, including data subjects' rights protection, security, and cross-border jurisdiction. Pre-PDP Law, regulations were fragmented, lacking certainty for cloud technology; the enactment of Law Number 27 of 2022 provided a comprehensive framework defining personal data, subjects' rights, controllers'/processors' duties, and transfer mechanisms. Implementation hurdles persisted, such as absent supervisory authorities, unprepared businesses, non-compliant foreign providers, weak derivative rules, and low digital literacy. Enhancements required establishing independent oversight, issuing regulations, boosting literacy, and fostering international cooperation. Future research should empirically assess PDP Law

compliance among cloud providers post-supervisory authority formation, evaluating enforcement efficacy through case studies.

REFERENCES

Alcácer, Juan, Cantwell, John, & Piscitello, Lucia. (2016). Internationalization in the information age: A new era for places, firms, and international business networks? *Journal of International Business Studies*, *47*(5), 499–512.

Attaran, Mohsen. (2017). Cloud computing technology: leveraging the power of the internet to improve business performance. *Journal of International Technology and Information Management*, *26*(1), 112–137.

Attaran, Mohsen, & Woods, Jeremy. (2019). Cloud computing technology: improving small business performance using the Internet. *Journal of Small Business & Entrepreneurship*, *31*(6), 495–519.

Banditwattanawong, Thepparit, Masdisornchote, Masawee, & Uthayopas, Putchong. (2016). Multi-provider cloud computing network infrastructure optimization. *Future Generation Computer Systems*, *55*, 116–128.

Bansah, Abednego Kofi, & Darko Agyei, Douglas. (2022). Perceived convenience, usefulness, effectiveness and user acceptance of information technology: evaluating students' experiences of a Learning Management System. *Technology, Pedagogy and Education*, *31*(4), 431–449.

Baybarin, Andrey, Afonin, M. V, Maksimenko, Elena Ivanovna, Goncharov, Vitaly V, & Singilevich, Dmitriy Aleksandrovich. (2020). Information security of Internet users: Technological and legal opportunities for personal protection. *EurAsian Journal of BioSciences*, *14*(2).

Brown, John Seely, & Duguid, Paul. (2017). *The social life of information: Updated, with a new preface*. Harvard Business Review Press.

Galperin, Hernan, & Fernanda Viecens, M. (2017). Connected for development? Theory and evidence about the impact of internet technologies on poverty alleviation. *Development Policy Review*, *35*(3), 315–336.

Groom, Frank M. (2018). The basics of cloud computing. In *Enterprise Cloud Computing for Non-Engineers* (pp. 1–42). Auerbach Publications.

Kamilaris, Andreas, & Pitsillides, Andreas. (2016). Mobile phone computing and the internet of things: A survey. *IEEE Internet of Things Journal*, *3*(6), 885–898.

Kiswani, Jalal H., Dascalu, Sergiu M., & Harris Jr, Frederick C. (2021). Cloud computing and its applications: A comprehensive survey. *International Journal of Computer Applications IJCA*, *28*(1), 3–24.

Lee, Chanhyuk, Kim, Jisoo, Ko, Heedong, & Yoo, Byounghyun. (2024). Addressing IoT storage constraints: A hybrid architecture for decentralized data storage and centralized management. *Internet of Things*, *25*, 101014.

Moura, Jose, & Hutchison, David. (2016). Review and analysis of networking challenges in cloud computing. *Journal of Network and Computer Applications*, *60*, 113–129.

Patterson, David A., & Hennessy, John L. (2016). *Computer organization and design ARM edition: the hardware software interface*. Morgan kaufmann.

Schnoll, Hans J. (2015). *E-Government: Information, Technology, and Transformation: Information, Technology, and Transformation*. Routledge.

Sciences, National Academies of, Medicine, Engineering, Division on, Sciences, Physical, Science, Computer, Board, Telecommunications, Technology,

Committee on Information, & Workforce, the U. S. (2017). *Information technology and the US Workforce: Where are we and where do we go from here?* National Academies Press.

Stergiou, Christos, & Psannis, Kostas E. (2017). Recent advances delivered by mobile cloud computing and internet of things for big data applications: a survey. *International Journal of Network Management*, *27*(3), e1930.

Sunyaev, Ali. (2020). Cloud computing. In *Internet computing* (pp. 195–236). Springer.

Volti, Rudi, & Croissant, Jennifer. (2024). *Society and technological change*. Waveland Press.

Yamin, Mohammad. (2019). Information technologies of 21st century and their impact on the society. *International Journal of Information Technology*, *11*(4), 759–766.