PANCASILA AND LAW REVIEW

Doktoral Ilmu Hukum, Fakultas Hukum, Universitas Lampung,
Bandar Lampung, Lampung, Indonesia.
Volume 6 Issue 1, January 2025: pp: 15-44
http://jurnal.fh.unila.ac.id/index.php/plr
P-ISSN: 2723-262X E-ISSN: 2745-9306

Legal Protection of Personal Data Against Phishing in Indonesia: A Pancasila-Based Approach

Gunsu Nurmansyah[1], Rudi Natamiharja[2], Ikhsan Setiawan[3]

[1]Universitas Bandar Lampung, Indonesia
E-mail: gunsu.nur@ubl.ac.id
[2]Universitas Lampung, Indonesia
E-mail: rudi.natamiharja@fh.unila.ac.id
[3]Universitas Sriwijaya, Indonesia
E-mail: ikhsanstwn17@gmail.com

Submitted:Apr 28, 2025 ; Reviewed:July 15, 2025 ; Accepted: August 20, 2025

Article's Information

Keywords:
Legal Protection; Personal Data Protection; Phishing Crimes; Cybersecurity.

DOI :
https://doi.org/10.25041/plr.v6i1.4138

Abstract

Phishing in Indonesia presents significant risks to privacy and data security. This study employs a normative juridical approach to analyze the protection of personal data, with attention to both preventive and repressive legal mechanisms. It assesses the effectiveness of Law No. 27 of 2022 on Personal Data Protection in combating phishing, alongside measures of digital literacy and law enforcement. The findings indicate notable progress but highlight persistent challenges in enforcement capacity, public awareness, and international cooperation. The study recommends strengthening enforcement, expanding cybersecurity education, and enhancing cross-border collaboration to advance data protection.

A. Introduction

The protection of privacy rights is a well-established principle of international law. Since the adoption of the Universal Declaration of Human Rights (UDHR) in 1948, privacy has been recognized as a core human right requiring legal safeguards. Article 12 of the UDHR prohibits arbitrary interference with one's privacy, family, or correspondence and guarantees legal

protection against such intrusions—a principle reaffirmed in Article 17 of the 1966 International Covenant on Civil and Political Rights (ICCPR).

As UN member states, Indonesia and other nations are obliged to implement national policies ensuring privacy protection. This obligation also operates at the regional level, as reflected in Article 21 of the 2012 ASEAN Human Rights Declaration, which guarantees protection against interference with privacy, including personal data, and safeguards honor and reputation.

Indonesia's legal framework reflects this commitment. Law No. 39 of 1999 on Human Rights addresses personal protection, while Article 28G(1) of the second amendment to the 1945 Constitution enshrines the right to personal and family integrity, honor, dignity, and security from threats. The enactment of Law No. 27 of 2022 on Personal Data Protection represents a significant milestone, providing comprehensive regulation of privacy as an integral element of human rights.[1]

The right to data privacy constitutes an integral component of the broader, inherent right to privacy afforded to every individual. Protection against the misuse of personal data has been recognized as a fundamental human right, enshrined in Article 12 of the 1948 Universal Declaration of Human Rights and further reinforced by its derivative provision, Article 17 of the 1966 International Covenant on Civil and Political Rights*)*[2].

Human rights are implemented differently across nations according to each country's ideological foundations and prevailing legal frameworks. Consequently, the perception and regulation of privacy vary from one jurisdiction to another. Schrems notes that privacy is closely tied to the social and cultural context of a country. For example, the United States and Europe adopt different privacy paradigms. European courts apply definitions that differ from the U.S. legal system, which focuses on the boundaries of what is considered reasonable privacy[3]. The understanding of privacy also differs depending on its domain. In some cultures, religious relationships are treated as private matters, whereas in others they are not. This diversity of perspectives indicates that privacy cannot be rigidly defined as right or wrong and cannot be determined solely through logical reasoning.[4]

The expansion of the digital economy has made big data, particularly aggregated data, an important economic asset in Indonesia. Communication patterns and consumer behavior are routinely recorded by network operators and digital platforms, making big data highly valuable and a resource that Indonesia needs to manage and utilize effectively. However, vulnerabilities in data protection have become increasingly apparent. Cybersecurity firm Surfshark reported that 1.04 million user accounts were breached in Indonesia during the second quarter of 2022,

[1] Rudi Natamiharja, M Stefany, 2019, "Perlindungan Hukum Atas Data Pribadi Di Indonesia (Studi Terhadap Pelaksanaan Pelayanan Jasa Telekomunikasi PT. Telekomunikasi Selular)", *Prodigy Jurnal Perundang undangan*, Volume 7 Issue 2, hlm. 3.

[2] Rudi Natamiharja dan Mindoria, Stefany, 2019, *Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN*, *Project Report*, Bandar Lampung : Aura.

[3] Jonathan Patrick, 2022, "Ahli: Big Data Jadi Komoditas Utama di Era Digital Indonesia", *https://www.cnnindonesia.com*. diakses pada 24 September 2023.

[4] The Max Schrems Litigation, "A Personal Account Mohini Mann dalam Elaine Fahey Editor Institutionalisation beyond the Nation State Transatlantic Relations: Data, Privacy and Trade Law Studies", *European Economic Law and Regulation*, Volume 10 hal. 76

P-ISSN 2723-262X
E-ISSN 2745-9306

representing a 143 percent increase compared to the 430,100 accounts breached in the first quarter. The Ministry of Communication and Information Technology recorded 35 cases of data breaches between January and June 2023, exceeding the total annual breaches recorded from 2019 to 2021.

According to DataIndonesia.id, several major breaches occurred in 2023. On 12 March, a user named "Bjorka" on Breach Forums claimed to have leaked the data of 19.56 million BPJS Employment customers. Lockbit announced the theft of 1.5 terabytes of personal data from Bank Syariah Indonesia users, demanding a ransom of 20 million U.S. dollars, equivalent to approximately 297 billion Indonesian rupiah, with a payment deadline of 15 May. In late June, Bjorka claimed to have hacked 35 million user records from MyIndiHome and offered the data for sale for 5,000 U.S. dollars, equivalent to about 752.65 million Indonesian rupiah. [5] This article was published on DataIndonesia.id under the title "List of Indonesia's Data Breach Cases in 2023, from BSI to Passports."

Technological developments have significantly contributed to the advancement of human civilization. Nevertheless, technology also functions as a double-edged sword, facilitating the emergence of unlawful activities in cyberspace, commonly referred to as cybercrime[6]. Since 2003, various forms of cybercrime have evolved as new criminal typologies driven by advances in information technology. These include carding (credit card fraud), ATM/EDC skimming, hacking, cracking, phishing (internet banking fraud), malware attacks (viruses, worms, trojans, bots), cybersquatting, pornography, online gambling, and transnational crimes such as drug trafficking, organized crime, terrorism, money laundering, human trafficking, and illicit economic activities[7].

Data from the e-MP Robinopsnal of the Criminal Investigation Department (Bareskrim Polri) indicate that between 1 January and 22 December 2022, Indonesian police handled 8,831 cybercrime cases involving all regional police departments (Polda) and units under Bareskrim. Polda Metro Jaya recorded the highest number of cases with 3,709, a sharp increase compared to the 612 cases reported nationwide in 2021. In the same period, law enforcement processed 8,372 individuals alleged to be involved in these crimes. As of the time of writing, official cybercrime statistics for 2023 and 2024 from Bareskrim Polri have not been made publicly available.[8]

---

[5] Shilvina Widi, 2023, "Deret Kasus Kebocoran Data RI pada 2023, dari BSI hingga Paspor", *https://dataindonesia.id/internet/detail/deret-kasus-kebocoran-data-ri-pada-2023-dari-bsi-hingga-paspor*, diakses pada tanggal 27 Agustus 2023

[6] A. Aco Agus dan Riskawati. 2016, "Penanganan Kasus Cybercrime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar)", *Jurnal Supremasi*, Vol. 10, N hlm. 56.

[7] Maulia Jayantina Islami, 2017, "Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index," *Jurnal Masyarakat Telematika Dan Informasi*, Vol. 8 No. hlm. 137.

[8] Pusiknas Bareskrim Polri, 2023, "Kejahatan Siber di Indonesia Naik Berkali-kali Lipat*",* *https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat*.

Figure 1. Increase in Cybercrime Cases in Indonesia over the Last 2 Years
Source: e-MP Robinopsnal Bareskrim Polri

www.patrolisiber.id releases that the Criminal Investigation Agency (Bareskrim Polri) represents the Directorate of Cybercrime (Dittipidsiber) responsible for law enforcement against cybercrime. The Directorate handled two categories of cyber-related crimes throughout 2022 (January – December 2022) as follows.[9]

No	Types of Cybercrime Cases	Number of Cases
1	Manipulation of authentic data	3.723
2	Fraud through electronic media	2.131
3	General cybercrime	1.098
4	Defamation through electronic media in the form of persecution	835
5	Illegal system access	358
6	Online gambling	164
7	Threats in the form of persecution	145
8	Pornography and prostitution through electronic media	143
9	Insult via electronic media	59
10	Hate speech through electronic media	43

Table 1. Types of Cybercrime Cases in Indonesia Most Frequently Occurring in 2022

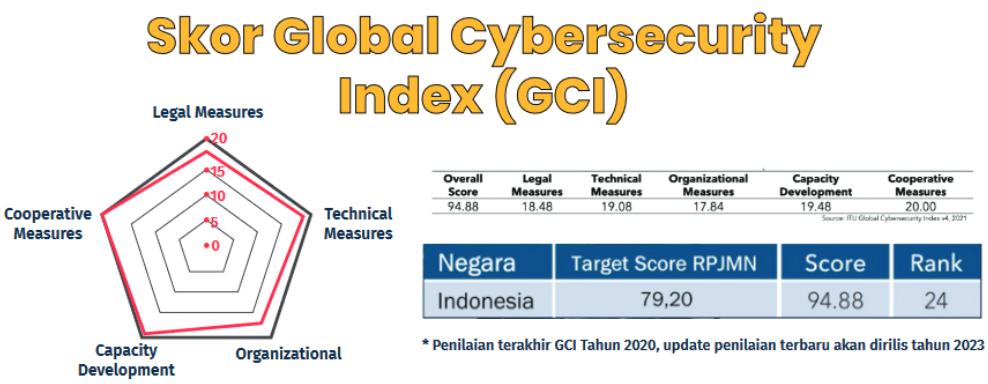
According to the ASEAN Cyberthreat 2021 data released by Interpol, Indonesia ranks first among ASEAN countries in malware-related cybercrime, recording approximately 1.3 million cases. This figure represents nearly half of all ransomware threats reported within the region. Vietnam ranks second with 886,874 cases, while Brunei records the lowest incidence with only 257 cases. Furthermore, the National Cyber Security Index (NCSI) places Indonesia sixth among ASEAN countries and 83rd out of 160 countries worldwide in terms of cybersecurity capacity.

The National Cyber and Crypto Agency (BSSN), in its 2022 Annual Report, provides further insights into the national cybersecurity landscape. Drawing on the most recent available data from the Global Cybersecurity Index (GCI) assessment in 2020, the report outlines Indonesia's cybersecurity index score as follows:

[9] *Ibid*

P-ISSN 2723-262X
E-ISSN 2745-9306

Figure 2. Indonesia's Position in the Global Cybersecurity Index (GCI) 2020 (Annual Report BSSN 2022, https://www.bssn.go.id)



In the context of preventive measures for personal data protection, a critical focus is the mitigation of phishing crimes, among the most damaging forms of cybercrime with significant societal impacts. Data from the Anti-Phishing Working Group (APWG) indicate a consistent annual rise in phishing-related incidents worldwide. APWG monitors global phishing trends by tracking the number of unique phishing sites reported via emails, drawing on submissions from international research partners and public reports to its website. In 2019, reported attacks averaged fewer than 100,000 unique phishing sites per month. This figure doubled to approximately 200,000 per month between 2020 and 2021, and in 2022 surged to 300,000–400,000 per month, peaking in December. The year 2022 marked a record high, with over 4.7 million attacks recorded, around 150% annual increase since early 2019. In the fourth quarter of 2022, the financial sector, particularly banking, was the most targeted industry, accounting for 27.7% of all phishing attacks.

The Phishing Activity Trends Report 4th Quarter 2022 shows that the phishing crimes worldwide reached its peak in 2022.

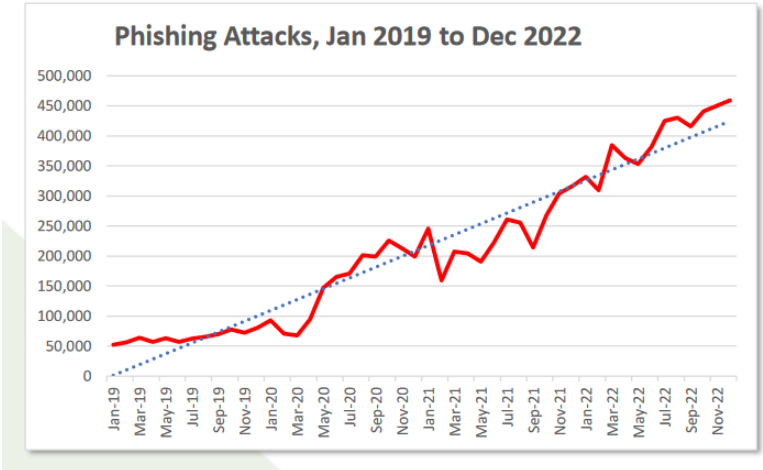


Figure 3. Phishing Activity Trends Report 4th Quarter 2022
Source: APWG Phishing Activity Trends Report, http://www.apwg.org

Phishing is a form of cybercrime that employs deception to obtain sensitive personal information by imitating legitimate entities through fraudulent websites or links. Victims are typically lured into providing data such as their full name, address, credit card number, and contact details, which perpetrators subsequently exploit for activities including social media account breaches and financial fraud. Such attacks often inflict long-term social and psychological harm. Originally prevalent in email-based schemes, phishing has evolved to target mobile devices and social media platforms, and is now facilitated by artificial intelligence (AI). Generative AI enables cybercriminals to craft highly convincing phishing content, accelerate malware development, and bypass authentication systems through synthetic images and voice imitations of targeted individuals[10].

Phishing causes both material and immaterial losses, primarily through the theft of personal data, leading to prolonged victimization. The impact extends beyond individuals to electronic systems, corporations operating such systems, and financial institutions serving as payment partners. Under Indonesian law, phishing is punishable pursuant to Law No. 19 of 2016 amending Law No. 11 of 2008 on Electronic Information and Transactions, and Law No. 27 of 2022 on Personal Data Protection[11].

This study focuses on legal protection of personal data against phishing crimes in Indonesia. The urgency of this issue has intensified amid rapid technological advancement in the Fourth Industrial Revolution, where the proliferation of digital technologies has resulted in unprecedented volumes of personal data being generated, stored, and disseminated through computers, websites, and social media[12].

B. Discussion

1. Regulation of Personal Data Protection in Indonesia

An analysis of Law No. 27 of 2022 on Personal Data Protection reveals that the protection of personal data is inherently linked to the concept of privacy to protect one's integrity and dignity.[13] The impetus for Indonesia's personal data protection legislation did not emerge from its indigenous legal traditions from international economic cooperation pressures. Specifically, Indonesia's commitment to the OECD Guidelines, signed in 2004, and adherence to the APEC Privacy Framework of 2004 prompted the adoption of privacy and data protection regulations. The latter explicitly emphasizes that the potential of electronic commerce depends on the joint

[10] Ensign rilis laporan soroti tren ancaman siber di Indonesia, 2023, *https://www.antaranews.com/berita/3664086/ensign-rilis-laporan-soroti-tren-ancaman-siber-di-indonesia*, diakses pada 27 Agustus 2023.
[11] Hariyono, A.G. and Simangunsong, F., 2023, "Perlindungan Hukum Korban Pencurian Data Pribadi (Phishing Cybercrime) Dalam Perspektif Kriminologi", *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance,* 3(1), pp.428-439.
[12] Shilling, C. G, 2011, "Privacy and Data Security: New Challenges of The Digital Age", *New Hampshire Bar Journal*, 52 (2): 28.
[13] Ministry of Communication and Informatics (Kementerian Komunikasi dan Informatika), *Naskah Akademik Rancangan Undang-Undang tentang Perlindungan Data Pribadi*, Jakarta: 2020, p. 16.

P-ISSN 2723-262X
E-ISSN 2745-9306

efforts of governments and businesses to address issues, including privacy, through appropriate technologies and policies[14].

While privacy is not a novel concept in Indonesian law, its historical regulation can be traced to the Staatsblad Royal Decision No. 36 of July 25, 1893, concerning the authority to detain and confiscate letters and documents at post offices that is one of the earliest legal provisions on communication privacy in the country[15].

Indonesia's regulation of privacy and personal data protection is not codified in a single statute but is grounded in Article 28G of the 1945 Constitution of the Republic of Indonesia. This article affirms that "Every person has the right to protection of themselves, their family, honor, dignity, and property under their control, as well as the right to feel safe and to be protected from threats of fear for doing or not doing something that is a human right." This constitutional safeguard serves as the primary legal basis for the development of specific personal data protection legislation in Indonesia[16].

The Telecommunications Law prohibits wiretapping and the interception of information transmitted through telecommunication networks. In the context of personal data processing in public spaces, the protection of personal data is recognized as a constitutional right, and its disclosure is restricted as exempt information under public information disclosure laws. According to a 2016 ELSAM study, at least 30 Indonesian regulations explicitly or implicitly address personal data protection[17].

The Law on Information and Electronic Transactions (UU ITE) plays a pivotal role in Indonesia's data protection framework by requiring the consent of the data subject as the legal basis for data processing. Unauthorized processing grants the data subject the right to seek compensation. During the amendment of the 2008 UU ITE, legislators and experts proposed additional safeguards, including the "right to be forgotten," enabling the deletion of irrelevant personal data.

The enactment of personal data protection laws aims to safeguard consumer interests and support Indonesia's economic growth. Such regulations reduce the risk of personal data misuse across sectors, including banking, online social networks (e.g., Facebook, MySpace, Twitter, Path, Google Plus), the national electronic ID card (e-KTP) program, and e-health systems. Risks arise from identity theft, targeted criminal activities, search engine indexing (e.g., Google, Bing), and cloud computing vulnerabilities. By addressing these threats, personal data protection legislation seeks to ensure both consumer security and economic stability[18].

Data protection affirms an individual's right to determine whether to share personal data and to set the conditions for its exchange. This principle is closely tied to privacy rights, which

[14] Wahyudi Djafar dan Asep Komarudin, 2014, *Perlindungan Hak Atas Privasi di Internet-Beberapa Penjelasan Kunci*, Jakarta: Elsam, hlm. 2
[15] S Yuniarti, AM Ramli, SD Rosadi, D Budhijanto. 2023, "The New Chapter Of Indonesia's Data Protection On Digital Economy Perspective", *Journal of Southwest Jiaotong University* 58 (3)
[16] Djafar, W., Sumigar, B.R.F., And Setianti, B.L. 2016, "Personal Data Protection in Indonesia-Policy Institutionalization Perspectives from a Human Rights Perspective", *Institute for Policy Research and Advocacy*, pp. 30-31.
[17] Dewan Perwakilan Rakyat, 2016, "Risalah Rapat Komisi I dari Dewan Perwakilan Rakyat Republik Indonesia" tanggal 14 Maret hlm.13.
[18] Naskah Akademik Undang-undang Perlindungan Data Pribadi, 2022.

encompass the authority to decide on the disclosure of personal information.[19] The unauthorized collection or dissemination of such data constitutes a violation of privacy.[20] Moreover, personal data possesses significant economic value, functioning as an asset or commodity. Judicial interpretations of the interplay between privacy rights and law enforcement suggest that the gravity of a criminal offense does not diminish the scope of privacy protections[21].

Legal provisions on personal data protection in Indonesia remain fragmented and sectoral, resulting in suboptimal and ineffective safeguards for personal data as an element of privacy. Violations of privacy rights related to personal data can occur both online and offline. Online threats include the mass collection of personal data ("digital dossiers"), direct selling, social media activities, the electronic ID card (e-KTP) program, the e-health program, and cloud computing. A digital dossier involves the large-scale aggregation of personal information through digital technologies, often conducted by private entities using internet-based tools, thereby infringing upon individuals' privacy rights[22].

Direct selling refers to marketing practices in which sellers approach consumers directly, often facilitated by the growth of the data bank industry. These data banks collect consumer information and sell it to companies, enabling businesses to acquire such data for marketing purposes[23].

Definitions of personal data vary. Black's Law Dictionary associates it with privacy rights, which encompass the freedom and independence of individuals, including protection from government interference in personal affairs. Personal data protection, in this context, refers to legal safeguards applied to the collection, registration, storage, use, and dissemination of such data[24].

From a scholarly perspective, personal data constitutes a form of privacy recognized in international and regional human rights instruments, including the Universal Declaration of Human Rights (UDHR) 1948, the International Covenant on Civil and Political Rights (ICCPR), and the European Convention on Human Rights (ECHR). David Banisar further categorizes privacy into four distinct types as follows.[25]

a. Information privacy.
b. Bodily privacy.
c. Communication privacy.
d. Territorial privacy.

---

[19] Human Rights Committee General Comment No. 16 .1988, "on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17)" *International Report*, 2013, hlm. 1-2.

[20] Kamus Besar Bahasa Indonesia memberikan pengertian privasi berarti kebebasan dan keleluasaan diri, Kamus Besar Bahasa Indonesia, 2001, Edisi 3, Departemen Pendidikan Nasional dan Jakarta: PT. Balai Pustaka.

[21] Thomas Yeon and Yuan Shang Mathilda Kwong, 2021, "Warrantless Searches of a Mobile Phone's Digital Contents and Privacy Interests in Hong Kong", *Common Law World Review* 50, no. 2–3 (2021): 95–102, https://doi.org/10.1177/14737795211010822.

[22] Daniel J. Solove. 2004, "The Digital Person. Technology and Privacy in the Information Age", *West Group Publication*, New York University Press. New York. hlm. 13-17.

[23] Lydia K. Saragih, 2020, "Perlindungan Hukum Data Pribadi terhadap Penyalahgunaan Data Pribadi pada Platform Media Sosial", *Jurnal Hukum De'rechtstaat*, Vol. 6, No. 2, hlm. 126-127.

[24] Marcy E.Peek. 2006, "Information Privacy and Corporate Power: Toward a Reimagination of Information Privacy Law", *Seton Hall Law Review*, Vol 37, hlm. 6-7.

[25] David Banisar and Simon davies, 1999, "Global trend in privacy protection: an International Survey of Privacy, Data Protection and Surveillance Law and Development", *Journal Computer & Information 1*, hlm.3-4.

P-ISSN 2723-262X
E-ISSN 2745-9306

Law No. 27 of 2022 on Personal Data Protection defines and outlines general concepts reflecting the principles, intentions, and purposes laid out in the provisions of the Law as follows:

a. Personal Data

Personal data refers to any information relating to an individual's life that can identify or potentially identify that individual, whether alone or in combination with other data, and whether processed through electronic or non-electronic systems. Under the Personal Data Protection Law, such data includes, but is not limited to, a person's name, date of birth, identification number, passport number, physical characteristics, fingerprints, marital status, family relationships, education, employment, medical records, healthcare history, genetic information, sexual life, health examinations, criminal records, contact details, financial status, social activities, and other information capable of directly or indirectly identifying a living person.

Law No. 14 of 2008 on Public Information Openness defines information as descriptions, statements, ideas, or signs containing values, meanings, and messages, whether in the form of data, facts, or explanations, that can be seen, heard, or read, and presented in any format in accordance with developments in information and communication technology, both electronic and non-electronic.

b. Sensitive personal data.

UK Data Protection Act 1998 mentions the categories of sensitive personal data:

a) Race or ethnic origin of the data subject;
b) Political opinions;
c) Religious beliefs or other similar beliefs;
d) Membership in trade unions;
e) Physical or mental health conditions;
f) Sexual life;
g) Criminal convictions or allegations of criminal activity;
h) Court proceedings related to any alleged criminal activity and the decisions made by the courts.

The National Personal Data Protection Law incorporates principles derived from international data protection standards. In line with the OECD Guidelines on Privacy Protection and Transborder Flows of Personal Data, Indonesia's data protection framework, both prior to and following the enactment of the Personal Data Protection Law, reflects consistency with international norms. Consequently, Indonesia's personal data protection principles are harmonized with global regulations[26].

The scope of the Personal Data Protection Law is extraterritorial, reflecting the borderless nature of data processing activities. Similar to the Law on Electronic Information and Transactions, it applies to data processing conducted both within and outside Indonesia when such activities have legal consequences in Indonesia or affect Indonesian citizens abroad. The primary object of regulation is personal data itself, which is classified as individual data as

[26] S Yuniarti, AM Ramli, SD Rosadi, D Budhijanto. 2023, *Op cit*. hlm 113.

previously described. The terminology used in the Personal Data Protection Law is consistent with that in Government Regulation No. 82 of 2012 on the Implementation of Electronic Systems and Transactions (PPPSTE). For coherence, the definition of personal data across various regulations should be aligned with the Personal Data Protection Law, namely information about an identified or identifiable individual, either on its own or in combination with other information, processed through electronic or non-electronic systems[27].

Law No. 27 of 2022 on Personal Data Protection meets subjective justice, as it aligns with the principles of OECD (Organization for Economic Cooperation and Development).

a) Limitation of Collection Principle: Limited and specific, lawful, and transparent.
b) Data Quality Principle: Accurate, complete, not misleading, up-to-date, dated, and accountable.
c) Limitation of Use Principle: Processing according to purpose; destroyed and/or deleted after the retention period or subject request, unless otherwise specified by law.
d) Security Protection Principle: Protecting the security of personal data from unauthorized access, disclosure, alteration, misuse, destruction, and/or negligence.
e) Transparency Principle: Informing the purpose, processing activities, and protection failures.
f) Individual Participation Principle: Guaranteeing rights over personal data of the subject.
g) Accountability Principle: Conducted responsibly and clearly evidenced

A legal instrument for protecting privacy over personal data in the digital economy era must meet several criteria:[28]

a. International Character of Privacy and Personal Data Protection

In the digital economy, data does not move physically to a predictable destination as in the traditional economy. In transactions between individuals and private companies, the physical location of stored personal data is often indeterminate, as digital storage is no longer confined to national jurisdictions and may be cross-border. Data can be accessed by parties in other countries beyond the data owner's jurisdiction. Effective protection therefore requires the adoption of cross-border regulations. Such regulations should stipulate that the transfer of personal data abroad must be subject to explicit consent and permitted only to jurisdictions with privacy and data protection standards equivalent to those of the originating country.

b. Privacy Protection of Data as a Binding Element for Individuals and the Economic Society. Privacy and personal data rights possess an international dimension due to their uncertain status within national legal systems. National legal protection raises two key perspectives. First, privacy functions as a right establishing boundaries between individuals and society. Second, particularly in the digital economy, privacy also operates as a right that binds individuals to the broader digital community. Robust privacy and personal data protection fosters individual confidence, enabling greater participation in the digital economy.[29]

[27] *Ibid*. hlm 114.
[28] Sinta Dewi Rosadi, 2018, "Perlindungan Privasi Dan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia", *Veritas et Justitia*, Volume 4 Nomor 1, hlm. 93.
[29] *Ibid.*

P-ISSN 2723-262X
E-ISSN 2745-9306

Indonesia's regulatory framework on privacy and personal data protection is dispersed across multiple statutes. These include Law No. 36 of 2009 on Health, which governs patient confidentiality; Law No. 10 of 1998 on Banking, which protects the privacy and personal data of bank customers; Law No. 36 of 1999 on Telecommunications; Law No. 39 of 1999 on Human Rights; Law No. 23 of 2006 on Population Administration, as amended by Law No. 24 of 2013; and Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016.

Other laws contain provisions related to personal data without explicitly or comprehensively ensuring its protection. Examples include Law No. 40 of 2014 on Insurance, Law No. 21 of 2011 on the Financial Services Authority, and Law No. 28 of 2007 on the Third Amendment to Law No. 6 of 1983 on General Provisions and Tax Procedures. The key statutory provisions specifically addressing personal data protection can be outlined as follows.

a. Law No. 14 of 2008 on Public Information Disclosure

Article 1(1) of the Public Information Disclosure Law defines information as explanations, statements, ideas, or signs containing value, meaning, and messages, whether in the form of data, facts, or interpretations, that can be seen, heard, or read, and presented in various formats in line with developments in information and communication technology, both electronic and non-electronic. Public information is defined as information produced, stored, managed, transmitted, or received by a public body in connection with the administration of the state or the activities of other public institutions for the public interest. The protection of data and public information collected by public agencies is regulated in Article 6(3) of the Public Information Disclosure Law. According to this provision, there is public information that cannot be provided by a public agency, including:

a) Information that could endanger the state;
b) Information related to the protection of business interests from unfair competition;
c) Information concerning personal rights;
d) Information regarding official secrets;
e) Public information that has not been acquired or documented

b. Law No. 7 of 1992 on Banking as amended by Law No. 10 of 1998 on Banking.

Article 40 of the Banking Law requires banks to maintain the confidentiality of depositor information and their deposits, except in circumstances expressly permitted by law. Customer privacy protection extends beyond financial data, such as savings or other banking products, to encompass personal data, including identity details and other non-financial personal information.

Chapter VII on Bank Secrecy, Articles 41 to 44 of Law No. 10 of 1998 on Banking, provides several exceptions to the obligation to maintain bank secrecy. These exceptions include:

a) For tax purposes, exceptions can be granted to tax officials upon the request of the Minister of Finance, with permission from the Bank Indonesia Governor (Article 41);

b) For the settlement of bank debts that have been transferred to the State Debt and Auction Affairs Agency (PUPN), exceptions can be granted to PUPN officials with permission from the Bank Indonesia Governor (Article 41A);
c) For judicial purposes in criminal cases, exceptions can be granted to police, prosecutors, or judges with permission from the Bank Indonesia Governor (Article 42);
d) In civil cases between a bank and its customer, exceptions can be granted without the need for Bank Indonesia Governor's approval (Article 43);
e) For information exchange between banks, exceptions can be granted without the need for Bank Indonesia Governor's approval (Article 44);
f) Upon the written request, consent, or power of attorney of the depositor, exceptions can be granted without the need for Bank Indonesia Governor's approval (Article 44A);
g) Upon the request of the lawful heirs of a deceased depositor (Article 44A(2)).

c. Law No. 36 of 1999 on Telecommunications.

Article 42 of Law No. 36 of 1999 on Telecommunications requires service providers to protect the confidentiality of customers' personal data and private information, including the content of communications sent or received through their networks. Disclosure is permitted only for judicial purposes in criminal cases, upon a written request from the Attorney General, the Chief of Police, or authorized investigators.

d. Law No. 8 of 1999 on Consumer Protection.

The Consumer Protection Law guarantees data and information related to goods and services, but not consumers' personal data. Article 2 sets out principles of benefit, fairness, balance, security, consumer safety, and legal certainty, without explicitly addressing personal data protection. In practice, consumer protection should also extend to safeguarding personal data and information.

e. Law of the Republic of Indonesia No. 19 of 2016 on Amendments to Law No. 11 of 2008 on Electronic Information and Transactions.

The protection of privacy rights under the Electronic Information and Transactions Law is explained in the explanation of Article 26, which defines personal rights as follows:

a) The right to enjoy personal life and be free from any disturbance.
b) The right to communicate with others without being subjected to spying or surveillance.
c) The right to monitor access to information about one's personal life and data.

The Personal Data Protection Law defines a "data controller" broadly to include individuals, legal entities, public institutions, and international organizations. As the party determining the purposes and methods of processing personal data, the data controller holds a central role and significant responsibility. Article 1(4) identifies three essential elements:

a) Indonesia adopts a comprehensive regulatory model that applies to the public sector, the private sector, and international organizations.

b) Data processing activities may be conducted individually or jointly.
c) The data controller is the entity that determines the purposes of data processing.

Personal data protection in Indonesia follows the legal hierarchy set out in Law No. 12 of 2011 on the Formation of Legislation. Government Regulation No. 82 of 2012, issued under Law No. 19 of 2016, assigns electronic system operators the responsibility to safeguard personal data integrity and to obtain the data owner's consent for its collection, use, and disclosure. However, this regulation does not detail the fundamental principles of personal data protection. These are elaborated in Ministerial Regulation No. 20 of 2016 (Permenkoinfo No. 20/2016), which protects personal data across all stages, including acquisition, collection, processing, analysis, storage, display, disclosure, transmission, dissemination, and destruction. Additional protection is found in sectoral regulations, such as those of Bank Indonesia and the Financial Services Authority (OJK) for consumer data.

The Personal Data Protection Law establishes a comprehensive framework, explicitly holding international organizations accountable as data controllers. Accountability rests with the institution rather than individuals such as board members, directors, or employees, who act solely under the institution's authority and instructions. Accordingly, employees engaged in data processing are not considered data controllers or processors in their own right[30].

This framework allows the legal protection of personal data in Indonesia to be assessed in two periods: before and after the enactment of the Personal Data Protection Law as shown in Table 2.

Table 2. Analysis of Personal Data Protection Regulation in Indonesia

No	Before PDP Law	Substance	Analysis
1.	Law No. 14 of 2008 on Public Information Disclosure	Article 1 Paragraph (1) regulates the definition of information and public information. Article 6 Paragraph (3) covers public information that cannot be provided by public bodies	Categorization of information and public information, and regulation of information protected by the law.
2.	Law No. 10 of 1998 on Banking	Article 40 on bank secrecy, where banks are required to keep the identity and deposits of customers confidential. Articles 41 to 44	Protection of customer privacy not only concerns financial data (deposits or other bank products) but also personal data related to

[30] Guidelines 07/2020, "on the Concepts of controller and processor in the RDPR Verion 2.1", *http://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf*, diakses 29 September 2023.

		provide exceptions to the obligation to maintain bank secrecy.	identity or other personal details beyond financial data.
3	Law No. 36 of 1999 on Telecommunications	Article 42 Paragraph (2) requires telecommunications providers to protect and maintain the confidentiality of users' personal and other private information.	Telecommunication service providers are obligated to protect personal information of their users.
4.	Law No. 8 of 1999 on Consumer Protection	Guarantees protection for information about goods and services, but not personal data of consumers.	There is no consumer protection regarding personal data and information.
5.	Law No. 19 of 2016 on Electronic Information and Transactions	Article 26 explains personal rights: the right to enjoy private life free from interference, the right to communicate without being spied on, and the right to monitor access to personal information	The law provides protection for personal rights and defines them in three aspects.
In the PDP Law			
1	General Provisions	Articles 1 and 2 define and set limits on personal data, information, and data processing.	The academic formulation reflects the principles, objectives, and purpose of the Personal Data Protection Law.
2	Management of Sensitive Personal Data	Articles 3-4, sensitive personal data includes information on religion/beliefs, health, physical and mental conditions, sexual life, financial data, education, and other	Specific types of data protected under this law are categorized, and definitions are provided for sensitive personal data or general personal data.

P-ISSN 2723-262X
E-ISSN 2745-9306

		personal data that may harm privacy	
3.	Rights of Data Owners	Articles 5-15 include the right to request access, request corrections and updates, destroy personal data, claim compensation for violations, and withdraw consent.	Adequate protection is provided for the privacy interests of data owners.
4	Exceptions to Personal Data Protection	Under certain circumstances, for legitimate reasons and as regulated by law, breaches of personal data protection may occur.	In addition to the types of data protected by the law, exceptions to protection are also regulated.
5	Obligations of Data Controllers	Several obligations for data controllers include obtaining consent, stopping data processing, announcing privacy policies, ensuring data security, providing access, correcting errors, and ensuring data accuracy.	Detailed provisions exist for the withdrawal of consent, halting data processing, and safeguarding personal data through security measures.
6	Transborder Flow of Personal Data	Articles 55-56 allow the transfer of personal data to other data controllers both within and outside the jurisdiction of the Republic of Indonesia.	The law provides international regulations or at least meets international standards, referencing documents like the OECD Guidelines, EC Directives, and the AFTA Privacy Framework as references for national legal norms.
7	Dispute Resolution and Sanctions.	Articles 57, 64, and 67 address dispute	Proportional sanctions are in place for

		resolution, administrative sanctions, and criminal sanctions.	violations of the provisions of this law.

The regulation of personal data protection in Indonesia shows that privacy safeguards have existed in earlier laws, particularly the Information and Electronic Transactions Law (ITE Law). However, the Personal Data Protection Law (PDP Law) provides a more comprehensive framework, explicitly holding international organizations accountable as data controllers.

An evaluation of the PDP Law's adequacy must consider the influence of the European Union's General Data Protection Regulation (GDPR), which serves as the global benchmark. The GDPR is built on core principles such as lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability. It also guarantees extensive rights for data subjects, including rights to access, rectify, erase, restrict processing, data portability, and object to processing.[31]

Indonesia's PDP Law (Law No. 27 of 2022) incorporates many of these principles. Article 4 outlines the rights of data subjects, reflecting provisions in Articles 12–22 of the GDPR. The PDP Law adopts data minimization by requiring that data be relevant and limited to its intended purposes, and it mandates accountability by obligating data controllers to ensure lawful and secure processing.[32]

While structurally aligned with the GDPR, the PDP Law is also shaped by Pancasila as its philosophical foundation. The principle of human dignity (Sila Kedua) supports personal autonomy and privacy; social justice (Sila Kelima) demands that data use avoid harm and inequality; and unity (Sila Ketiga) reflects a preference for societal harmony, which may influence the balance between individual rights and collective or state interests.

Tensions can emerge when GDPR principles, rooted in individual autonomy and liberal rights, encounter Pancasila-based values that place collective interests above individual claims. For instance, while the GDPR upholds an almost absolute right to data erasure (the "right to be forgotten"), the PDP Law allows exceptions for reasons such as national security or public order—reflecting Pancasila's emphasis on societal harmony and national resilience.[33] Consequently, although the PDP Law mirrors the GDPR in form and structure, its normative foundation is distinct. It offers a legal model that integrates universal data protection standards with Indonesia's constitutional philosophy, demonstrating how global norms can be localized through Pancasila-based interpretation.

[31] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), OJ L 119/1, 4 May 2016.
[32] Law No. 27 of 2022 concerning Personal Data Protection, State Gazette of the Republic of Indonesia Year 2022 Number 210.
[33] Deni S. Mahmud, "The Influence of GDPR on Indonesian Data Protection Law," *Indonesian Journal of Law and Society*, Vol. 2, No. 1 (2023): 45–63.

P-ISSN 2723-262X
E-ISSN 2745-9306

2. Forms of Legal Protection of Personal Data Against Phishing Crimes in Indonesia

In the digital era, personal data functions as a valuable asset and a high-economic commodity that requires proper protection.[34] Although digitalization provides many benefits, it also creates new challenges in the context of the Fourth Industrial Revolution. The rapid development of information and communication technologies, which involves the collection, storage, processing, production, and transmission of data, has not been accompanied by sufficient legal safeguards in Indonesia. Existing regulations are still scattered across different laws and have not fully embodied the principles of personal data protection. Law No. 27 of 2022 on Personal Data Protection (PDP Law) provides Indonesia's first comprehensive framework for regulating personal data.[35] The forms of legal protection under the PDP Law can be outlined as follows.

a. Types of Personal Data

Article 1 paragraph 1 of the PDP Law defines personal data as information relating to an identified or identifiable living individual, such as names, passport numbers, photographs, phone numbers, email addresses, fingerprints, or DNA profiles, the disclosure of which may harm privacy rights. The law divides personal data into two categories, namely general and specific (sensitive) personal data. General personal data include identifiers such as an electronic ID (KTP-el), passport, or driver's license. Specific personal data include biometric and genetic information, criminal records, children's data, health information, and sensitive financial data. Article 4 paragraph 2 stipulates that the processing of specific personal data requires explicit consent due to the higher level of risk involved[36].

b. Rights of the Data Subject.

The PDP Law places data subjects at the center of protection by granting them control over the processing of their personal information. Article 20 paragraph 1 guarantees fundamental rights, including the right to transparency regarding data use, the right to correction of inaccurate data, and the right to restrict processing. These provisions emphasize that protection is not only achieved by imposing obligations on data controllers but also by empowering individuals to determine how their data is processed.

c. Personal Data Processing

The PDP Law defines processing as any operation performed on personal data for a specific purpose. Processing includes determining the role of the data controller, identifying the legal basis for processing, applying the principle of purpose limitation, minimizing the scope of collected data, and assessing risks to the data subject. Processing activities may serve more than one purpose. For example, storing an email address may be used both for user authentication and for marketing communication. When consent for one purpose is withdrawn, processing for the other purpose may still continue.

---

[34] Sanusi, M. Arsyad, 2004, *Teknologi Informasi & Hukum E-Commerce*. Jakarta: PT. Dian Ariesta, hlm.9.

[35] Elnizar, Normand Edwin, 2019. "Perlindungan Data Pribadi Tersebar di 32 UU, Indonesia Perlu Regulasi Khusus", Retrieved Februari 5, 2020. *https://www.hukumonline.com/berita/baca/lt5d1c3962e01a4/perlindungan-data-pribadi-tersebar-di-32-uu--indonesia-perlu-regulasi-khusus.*

[36] Sinta Dewi Rosadi, 2023, *Pembahasan UU perlindungan Data Pribadi (UU RI Nomor 27 Tahun 2022)*, Jakarta: Sinar Grafika, hlm 48.

The law stipulates that personal data processing consists of several activities, including obtaining, recording, or storing data; organizing, adapting, or altering data; retrieving data; disclosing data; and aligning, combining, erasing, or destroying data. Personal data processing must be carried out with strict regulation to prevent unauthorized access, disclosure, alteration, misuse, destruction, or deletion. The security of personal data seeks to address three interrelated dimensions, namely confidentiality, integrity, and availability (CIA), all of which must be ensured to maintain effective protection. Information security governance plays a crucial role in mitigating or avoiding risks arising from potential threats[37].

Government initiatives to strengthen personal data protection represent an important step toward safeguarding individual rights. Nevertheless, the rapid advancement of technology has also accelerated the sophistication of phishing crimes. According to the Phishing Activity Trends Report, Q4 2022 published by APWG and OpSec Security, phishing attacks on the financial sector remained the largest category, accounting for 27.7 percent of all incidents, an increase from 23.2 percent in the previous quarter. Webmail and Software as a Service (SaaS) providers were the second-most targeted sector at 17.7 percent, followed by payment processors such as PayPal, Venmo, and VISA at 6 percent. Attacks on social media companies fluctuated between 8.5 percent in Q4 2021 and 15.5 percent in Q2 2022 before declining, while phishing related to cryptocurrency exchanges and wallets decreased from 4.5 percent in Q2 to 2.3 percent in Q4 amid market volatility.[38]

Phishing websites typically impersonate trusted third parties such as banks or e-commerce platforms to deceive users into disclosing sensitive information. The main objective is to obtain credentials and personal information, including passwords, PINs, and financial account details, either for immediate exploitation or for resale to third parties. Attackers continuously innovate to bypass anti-phishing mechanisms, which underscores the need for advanced countermeasures. Intelligent detection systems based on web mining and machine learning are increasingly recognized as effective strategies for identifying and preventing phishing attempts[39].

Phishing represents a significant cybersecurity threat that exploits user trust by imitating legitimate online entities. It can be conceptualized as a classification problem, where website features are analyzed to distinguish malicious sites from legitimate ones. The information obtained through phishing often encompasses personal identity data, account credentials, and financial information, which may subsequently be misused for fraudulent activities or unauthorized transactions. [40]

---

[37] Paul Voht. "The worlds Biggest data Breaches", *http: //www.thalesgroup.com/en/markets/ digital-identity-and-security/magazine/worlds-biggest-data-breaches*, dalam Sinta dewi rosadi, diakses 10 Oktober 2023

[38] APWG Phishing Activity Trends Report, 2022, "Phishing Activity Trends Report, 4th Quarter 2022, *https://apwg.org*, *diakses 28 Agustus 2023*

[39] H. Zuhir, A.Selmat and M. Salleh, 2015, "The Effect of Feature Selection on Phish Website Detection an Empirical Study on Robust Feature Subset Selection for Effective Classification", *International Journal of Advanced Computer Science and Applications*, vol.6, no.10, pp. 221-232.

[40] *https://www.djkn.kemenkeu.go.id/kpknl-purwakarta/baca-artikel/14851/Waspada-Kehajatan-Phising-Mengintai-Anda.html*. diakses pada 28 Agustus 2023.

P-ISSN 2723-262X
E-ISSN 2745-9306

a) Email Phishing
   As the name suggests, email phishing uses email as a medium to reach potential victims. There are an estimated 3.4 billion fake emails sent every day. You can imagine how many victims might fall prey to this action.
b) Spear Phishing
   Spear phishing is a type of email phishing. Unlike mass email phishing, spear phishing targets specific victims. This technique is usually employed after gathering basic information about the victim, such as their name and address.
c) Whaling
   Whaling is a form of phishing that specifically targets individuals with high authority within an organization, such as business owners, company directors, HR managers, and others. If successful, whaling can provide significant benefits due to the access gained.
d) Web Phishing
   Web phishing involves creating fake websites to deceive potential victims. These phishing websites resemble legitimate websites and use similar domain names. This is known as domain spoofing.

Phishing recognition is often approached as a classification problem within data mining, where the objective is to predict whether a website is legitimate or malicious based on features in a training dataset. This dataset consists of website characteristics and their corresponding classification labels, allowing the model to learn patterns that distinguish legitimate websites from phishing attempts[41].

The use of Artificial Intelligence (AI) in phishing prevention has therefore become essential. Phishing crimes, which involve fraudulent attempts to acquire sensitive information such as passwords or credit card numbers through deception and social engineering, pose increasingly serious risks in the digital era. While technological solutions such as AI enhance detection, legal measures remain crucial to strengthen prevention and ensure accountability. The presence of legal instruments enables governments to take preventive action before phishing causes harm to individuals.

Phishing prevention must be closely integrated with personal data protection. Law No. 27 of 2022 on Personal Data Protection provides the legal framework for regulating the collection, use, and storage of data, including that processed by AI systems. Clear legal guidelines are vital to prevent misuse of personal data and to safeguard individual privacy. Thus, while personal data protection laws enhance the effectiveness of phishing prevention, they must simultaneously prioritize the protection of individual rights.

Legal protection against phishing crimes under the PDP Law can be realized through the implementation of personal data protection principles that align with international standards, including those outlined in the OECD Guidelines on privacy protection and cross-border data flows. The PDP Law provides comprehensive provisions on the classification of personal data,

[41] N. Abdelhamid, A. Ayesh and F. Thabtah, 2014, "Phishing Detection based Associative Classification Data Mining", *Expert System with Applications*, vol.41(13), pp.5948-5959,

the rights of data subjects, and the security of data processing. These provisions function as instruments not only to protect personal data but also to reduce the risks posed by phishing.

Legal protection is fundamentally a mechanism to safeguard legal subjects through statutory provisions. In the context of personal data, such protection under the PDP Law extends beyond regulating rights and obligations. It also ensures enforcement through sanctions, thereby providing both preventive and repressive measures. Legal protection under this law can therefore be understood in two main forms.

a. Preventive Legal Protection

   Preventive legal protection aims to minimize the risk of personal data misuse before violations occur. Provisions on preventive protection can be found in several sectoral laws enacted prior to the Personal Data Protection Law. For example, Law No. 10 of 1998 on Banking requires the confidentiality of customer data, including identity and other non-financial information. Law No. 36 of 1999 on Telecommunications obliges service providers to maintain the confidentiality of user data, while Law No. 19 of 2016 on Information and Electronic Transactions explicitly regulates and prioritizes privacy rights. Law No. 27 of 2022 further strengthens preventive protection through provisions on the management of sensitive personal data, obligations of data controllers, and regulation of cross-border data flows.

b. Repressive Legal Protection

   Repressive legal protection functions as the final safeguard after a violation has occurred, primarily through the imposition of sanctions. Law No. 27 of 2022 provides for administrative, civil, and criminal sanctions. Articles 57, 64, and 67 regulate dispute resolution, administrative measures, and criminal penalties, which may include fines, imprisonment, and compensation. Dispute resolution mechanisms are available both through out-of-court settlements, which must be undertaken voluntarily, and through court proceedings if non-judicial mechanisms fail.Accordingly, legal protection of personal data against phishing crimes in Indonesia can be categorized into preventive measures, which emphasize the protection of sensitive data, confidentiality obligations, and cross-border data control, and repressive measures, which emphasize sanctions and dispute resolution.

Despite these legal protections, societal attitudes toward privacy present a major challenge. As Westin observes, the human need for privacy is universal and has existed since primitive societies, where individuals sought personal space and boundaries to protect themselves[42]. However, perceptions of privacy are shaped by cultural, philosophical, and political contexts. In Indonesia, the communal character of society has historically placed less emphasis on individual privacy. Consequently, public awareness and appreciation of privacy remain limited, creating opportunities for misuse of personal data.

The enactment of the Personal Data Protection Law reflects the principle of legal protection in a state governed by law, which is bound to uphold justice, utility, and legal certainty. Nonetheless, from a sociological perspective, legal reform alone is insufficient. Effective

[42] Alan F. Westin (Editor), 1971, *Information Technology in a Democracy*, Massachusetts: Harvard University Press, hlm. 1.

P-ISSN 2723-262X
E-ISSN 2745-9306

protection requires cultural transformation through continuous public education and the development of normative values that recognize privacy as a fundamental human right, rather than merely an imported concept.

3. Conclusion

The protection of personal data in Indonesia, particularly against phishing, has become increasingly urgent in the digital era. Although Law No. 27 of 2022 on Personal Data Protection establishes a comprehensive framework, its implementation faces substantive and practical challenges. The law adopts principles from the European Union's GDPR, including data subject rights, data minimization, and accountability, thereby embedding a rights-based approach to data governance. At the same time, it reflects Pancasila values, which emphasize social justice, human dignity, and national unity.Combining international norms with Indonesia's constitutional philosophy offers both opportunities and tensions. It affirms universal privacy rights while requiring contextual adaptation to a collectivist society and legal culture. Persistent phishing crimes, fueled by low public awareness and institutional gaps, underscore the need to complement normative provisions with preventive measures, digital literacy, and cross-border cooperation.

For the PDP Law to function as an effective safeguard against cybercrime, Indonesia must reinforce enforcement mechanisms, ensure institutional accountability, and harmonize its framework with both global standards and Pancasila-based ethics. Future reforms should advance not only legal certainty but also the recognition of data protection as a constitutional and human right in the digital age.

Acknowledgments

Sincere gratitude is extended to all who contributed to the completion of this research. The valuable support and resources provided throughout the process made this work possible. Appreciation is also expressed for the opportunity that was given to explore and develop the ideas presented herein.

References

A. Journal

A. Aco Agus dan Riskawati. 2016, "Penanganan Kasus Cybercrime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar)", *Jurnal Supremasi*, Vol. 10.

Alexandra Gronow, 2021, "Identifying Victims of Sexual Harassment in the Age of #MeToo: Time for the Media to Prioritise a Victim's Right to Privacy", *Alternative Law Journal* 46, no. 2 (2021): 120–27, *https://doi.org/10.1177/1037969X211003681*.

Andrea M. Matwyshyn, 2005, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Pegulation*, Berkeley Business Law Journal 3, no. 1 (2005): 129.

Ardi Saputra Gulo, Sahuri Lasmadi, Kabib Nawawi, 2020, "Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik*", PAMPAS: Journal Of Criminal*, Volume 1 Nomor 2.

Arief Sidharta, 2004, "Kajian Kefilsafatan tentang Negara Hukum", *Jentera (Jurnal Hukum), Rule of Law, Pusat Studi Hukum dan Kebijakan (PSHK)*, Jakarta, edisi 3 Tahun II, November.

Branscomb, Information is the Lifeblood that sustain political, social and business decision, dalam Anne W. Branscomb, "Global Governance of Global Networks: A survey of Transborder Data Flows in Transition", *Vanderbilt Law Review*, Vol. 36, 1983, hlm. 985.

Case No D-, 2012, "The Royal Bank of Scotland Group Plc", *International Directory of Company Histories 904736*, no. 2012 (2020): 1–5.

Criminal Practice Report, 2023, "Phishing", no. 9 (2023): 1–2.

Daniel J. Solove. 2004, "The Digital Person. Technology and Privacy in the Information Age", *West Group Publication*, New York University Press. New York.

David Banisar and Simon davies, 1999, "Global trend in privacy protection: an International Survey of Privacy, Data Protection and Surveillance Law and Development", *Journal Computer & Information 1*.

Dewan Perwakilan Rakyat, 2006-2013, UU No.23/2006 tentang Administrasi Kependudukan, UU No.24/2013 tentang Perubahan Atas UU No.23/2006, dan UU No.23/2006 tentang Administrasi Kependudukan, dan UU No.14/2008 tentang Keterbukaan Informasi Publik.

Diniyah, K.J., 2022, "Perlindungan Hukum Bagi Korban Tindak Pidana Cyber Crime Phishing", *Dinamika*, 28(5), pp.3756-3775.

Djafar, W., Sumigar, B.R.F., And Setianti, B.L, 2016, "Personal Data Protection in Indonesia-Policy Institutionalization Perspectives from a Human Rights Perspective", *Institute for Policy Research and Advocacy*

Dewan Perwakilan Rakyat, 2016, "Risalah Rapat Komisi I dari Dewan Perwakilan Rakyat Republik Indonesia" tanggal 14 Maret.

Dewi, Sinta, 2015, "Privasi atas Data Pribadi: Perlindungan Hukum dan Bentuk Pengaturan diIndonesia", *Jurnal De Jure* 15 (2): 165.

Edmon Makarim, 2003, *Kompilasi Hukum Telematika*, PT. Raja Grafindo Perkasa, Jakarta hlm. 3. Lihat juga M. Arsyad Sanusi, *Teknologi Informasi & Hukum E-commerce*, PT. Dian Ariesta : Jakarta, 2004, hlm. 9. Menurut Branscomb, Information is the Lifeblood that sustain political, social and business decision, dalam "Anne W. Branscomb, Global Governance of Global Networks: A survey of Transborder Data Flows in Transition", *Vanderbilt Law Review*, Vol. 36, 1983.

P-ISSN 2723-262X
E-ISSN 2745-9306

E. Fernando Siregar, H. Helvis, and M. Markoni, "Analisa Yuridis Eksekusi Sita Jaminan Terhadap Tindak Pidana Pencucian Uang (TPPU) First Travel," *Jurnal Syntax Transformation*, vol. 2, no. 11, pp. 1560–1573, Nov. 2021, doi: 10.46799/jst.v2i11.454.

Erna P, 2019, "Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online (The Urgency of Personal Protection in Peer to Peer Lending)", *Majalah Hukum Nasional*, No.2.

Gary D Brown and Andrew O. Metcalf, 2014, "Easier Said than Done: Legal Reviews of Cyber Weapons", *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.2400530.

Graham Greenleaf, 2011, *Global Data Protection Laws*, Privacy Laws and Business Special Report, September.

Hanifan N, 2020, "Perlindungan Data Pribadi Sebagai Bagian Hak Asasi Manusia Atas Perlindungan Diri pribadi Suatu Tinjauan Komparatif Dengan Peraturan Perundang-undangan Di Negara Lain", *Selisik*, Vol.6 No.1. Hlm 2685-6816

Hariyono, A.G. and Simangunsong, F., 2023, "Perlindungan Hukum Korban Pencurian Data Pribadi (Phishing Cybercrime) Dalam Perspektif Kriminologi", *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, 3(1).

Human Rights Committee General Comment No. 16 .1988, "on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation" (art. 17) seperti yang dikutip dalam *Privacy International Report*, 2013

Hsuan Ting Chen, 2018, "Revisiting the Privacy Paradox on Social Media With an Extended Privacy Calculus Model: The Effect of Privacy Concerns, Privacy Self-Efficacy, and Social Capital on Privacy Management", *American Behavioral Scientist* 62, no. 10 (2018): 1392–1412, *https://doi.org/10.1177/0002764218792691*.

H. Zuhir, A.Selmat and M. Salleh, 2015, "The Effect of Feature Selection on Phish Website Detection an Empirical Study on Robust Feature Subset Selection for Effective Classification", *International Journal of Advanced Computer Science and Applications*, vol.6, no.10, 1 https://www.onetrust.com/blog/principles-of-privacy-by-design/

Isaac Taylor, 2017, "Data Collection, Counterterrorism and the Right to Privacy", *Politics, Philosophy and Economics 16*, no. 3 (2017): 326–46, *https://doi.org/10.1177/1470594X17715249*,

Joesoef, I. E, 2021, "Legal Protection of Personal Data against Customers in Technology. Based Money Lending Services", *International Journal of Social Science and Human Research*, 04(08). *https://doi.org/10.47191/ijsshr/v4-i8-01*.

Kyu Ho Youm and Ahran Park, 2016, "The Right to Be Forgotten in European Union Law: Data Protection Balanced with Free Speech?", *Journalism and Mass Communication Quarterly 93*, no. 2 (2016): 273–95, https://doi.org/10.1177/1077699016628824.

Lydia K. Saragih, 2020, "Perlindungan Hukum Data Pribadi terhadap Penyalahgunaan Data Pribadi pada Platform Media Sosial", *Jurnal Hukum De'rechtstaat,* Vol. 6, No. 2.

M. Al-diabat, 2016, "Detection and Prediction of Phishing Websites using Classification Mining Techniques", *International Journal of Computer Applications,* vol.147, no.5, pp.5-11.

Marcy E.Peek, 2006, "Information Privacy and Corporate Power: Toward a Reimagination of Information Privacy Law", *Seton Hall Law Review,* Vol 37.

Marta Otto, 2015, "The Right to Privacy in Employment: In Search of the European Model of Protection", *European Labour Law Journal* 6, no. 4 (2015): 343–63, https://doi.org/10.1177/201395251500600404.

Maulia Jayantina Islami, 2017, "Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index," *Jurnal Masyarakat Telematika Dan Informasi*, Vol. 8.

N. Abdelhamid, A. Ayesh and F. Thabtah, 2014, "Phishing Detection based Associative Classification Data Mining", *Expert System with Applications*, vol.41(13), pp.5948-5959

Nadezhda Purtova, 2010, "Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights", *Netherlands Quarterly of Human Rights 28*, no. 2 (2010): 179–98, *https://doi.org/10.1177/016934411002800203*.

Oleg Gennadievich Danilyan, Alexander Petrovich Dzeban, Yury Yurievich Kalinovsky, Eduard Anatolievich Kalnytskyi Et Svetlana Borisovna Zhdanenko, "Personal Information Rights And Freedoms Within The Modern Society", *Informatologia,* 30 Juin 2018, Volume 51, Nomor 1-2.

Pamungkas, W.C. and Saputra, F.T., 2020, "Analisa Mobile Phishing Dengan Incident Response Plan dan Incident Handling*, JURIKOM (Jurnal Riset Komputer)*, 7(4).

Rudi Natamiharja, 2018, "A Case Study on Facebook Data Theft in Indonesia", *Fiat Justisia: Jurnal Ilmu Hukum,* Volume 12 Issue 3.

Rudi Natamiharja, M Stefany, 2019, "Perlindungan Hukum Atas Data Pribadi Di Indonesia (Studi Terhadap Pelaksanaan Pelayanan Jasa Telekomunikasi Pt. Telekomunikasi Selular", *Prodigy Jurnal Perundang undangan*. Volume 7 Issue 2.

Rosadi, SD, 2017, "Implikasi Penerapan program E-Health Dihubungkan Dengan Perlindungan Data Pribadi", *Arena Hukum,* Vol.9 No.3

Sautunnida, L, 2018, "Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia;Studi perbandingan Hukum Inggris dan Malaysia", *Kanun Jurnal Ilmu Hukum,* Vol. 20 No.2

Siallagan, H, 2016, *"Penerapan Prinsip Negara Hukum Di Indonesia, Sosiohumaniora"*, 18(2), 122–128. https://doi.org/10.24198/SOSIOHUMANIORA.V18I2.9947.

P-ISSN 2723-262X
E-ISSN 2745-9306

Shilling, C. G. 2011, "Privacy and Data Security: New Challenges of The Digital Age", *New Hampshire Bar Journal*, 52 (2): 28.

Slamet Suhartono, 2019, "Hukum Positif Problematik Penerapan Dan Solusi Teoritiknya", *DiH: Jurnal Ilmu Hukum* 15, no. 2 (2019): 201–11, https://doi.org/10.30996/dih.v15i2.2549.

Suhail Amin Tarafdar and Michael Fay, 2018, *Freedom of Information and Data Protection Acts,* InnovAiT: Education and Inspiration for General Practice 11, no. 1 (2018): 48–54, https://doi.org/10.1177/1755738017735139.

S Yuniarti, AM Ramli, SD Rosadi, D Budhijanto, 2023, "The New Chapter Of Indonesia's Data Protection On Digital Economy Perspective", *Journal of Southwest Jiaotong University* 58 (3).

Sinta Dewi Rosadi, 2018, "Perlindungan Privasi Dan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia", *Veritas et Justitia,* Volume 4 Nomor 1.

Stephen J. Schulhofer, 2016, "An international right to privacy? Be careful what you wish for", *International Journal of Constitutional Law*, Vol. 14.

The Max Schrems Litigation, "A Personal Account Mohini Mann dalam Elaine Fahey Editor Institutionalisation beyond the Nation State Transatlantic Relations: Data, Privacy and Trade Law Studies", *European Economic Law and Regulation*, Volume 10.

Thomas Yeon and Yuan Shang Mathilda Kwong, 2021, "Warrantless Searches of a Mobile Phone's Digital Contents and Privacy Interests in Hong Kong", *Common Law World Review* 50, no. 2–3 (2021): 95–102, https://doi.org/10.1177/14737795211010822.

Wahid, A., 2018, "Keadilan Restoratif: Upaya Menemukan Keadilan Substantif?", *Jurnal Hukum Responsif,* 5(5), 1 M.Yasir Said and Yati Nurhayati, 2021, "A Review on Rawls Theory of Justice", *International Journal of Law, Environment,* and Natural Resources 1, no. 1; 29–36,

Wibowo, M.H. and Fatimah, N., 2017, "Ancaman phishing terhadap pengguna sosial media dalam dunia cyber crime", *JOEICT (Jurnal of Education and Information Communication Technology)*, 1(1), pp.1-2

B. Book

Andi Hamzah. 2015 ,*Delik-Delik Tertentu (Speciale Delicten) Didalam KUHP* Edisi Kedua, Jakarta:Sinar Grafika.

Alan F. Westin (Ed), 1971, *Information Technology in a Democracy,* Massachusetts: Harvard University Press.

Arif, B. N. 2005, *Pembaharuan Hukum Pidana Dalam Perspektif Kjian Perbandingan*. Bandung: Citra Aditya Bakti

Bagir Manan, 2004, *Hukum Positif Indonesia (Satu Kajian Teoritik),* Jakarta:FH UII Press.

Bayu Sujadmiko, 2017, *Pengantar Hukum Teknologi Informasi Internasional*, Bandar Lampung: Zam-zam Tower.

Daniel J. Solove, 2004, *The Digital Person. Technology and Privacy in the Information Age*, West Group Publication, New York: New York University Press.

Deddy Ismatullah dan Asep A. Sahid Gatara Fh, 2017, *Ilmu Negara: Dalam Multiperspektif Kekuasaan, masyarakat, Hukum dan Agama*, Bandung: Pustaka Setia.

Edmon Makarim. 2003, *Kompilasi Hukum Telematika*, Jakarta: PT. Raja Grafindo Perkasa.

Edmon Makarim, 2010, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*, Jakarta: Rajawali Pers.

European Union Agency for Fundamental Rights and Council of Europe, 2014, Handbook on European Data Protection Law, Belgium.

J Wagner DeCew, 1997, *In Pursuit of Privacy: Law, Ethics and the Rise of Technology*, Ithaca: Cornell University Press.

Kamus Besar Bahasa Indonesia memberikan pengertian privasi berarti kebebasan dan keleluasaan diri, Kamus Besar Bahasa Indonesia. 2001, Edisi 3, Departemen Pendidikan Nasional, Jakarta: PT. Balai Pustaka.

Lili Rasjidi dan I.B Wysa Putra, 2010, *Hukum Sebagai Suatu Sistem*, Bandung: Remaja Rusdakarya.

M. Arsyad Sanusi, 2004, *Teknologi Informasi & Hukum E-commerce*, Jakarta: PT. Dian Ariesta.

Moh Kusnadi dan Bintan R. Saragih, 2008, *Ilmu Negara*, Jakarta: Gaya Media Partama.

Muchsin, 2003, *Perlindungan dan Kepastian Hukum bagi Investor di Indonesia*, Surakarta: Universitas Sebelas Maret.

Muhammad Tholhah Hasan, 2001, *Perlindungan Terhadap Korban Kekerasan Seksual (Advokasi atas Hak Asasi Perempuan)*, Bandung: PT. Refika Aditama.

Natamiharja, Rudi and Mindoria, Stefany, 2019, *Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN*, Project Report. Bandar Lampung: Aura.

Phillipus M. Hadjon, 1987, *Perlindungan Hukum Bagi Rakyat Indonesia*, Surabaya: PT Bina Ilmu.

Sanusi, M. Arsyad, 2004, *Teknologi Informasi & Hukum E-Commerce*. Jakarta:PT. Dian Ariesta.

Satjipto Raharjo, 2000, *Ilmu Hukum*, Bandung: PT Citra Aditya Bakti.

P-ISSN 2723-262X
E-ISSN 2745-9306

Schoeman, F. D (Ed), 1984, *Philosophical Dimensions of Privacy: an Anthology*, Cambridge: Cambridge University Press.

Sinta Dewi Rosadi, 2023, *Pembahasan UU Perlindungan Data Pribadi (UU RI Nomor 27 Tahun 2022)*, Jakarta:Sinar Grafika.

Shinta Dewi, 2009, *Cyberlaw Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional*, Bandung : Widya Padjadjaran.

Soeroso, 2006, *Pengahantar Ilmu Hukum*, Cetakan Kedelapan, Jakarta: Sinar Grafika.

Setiono, 2004. Supremasi Hukum, Surakarta: UNS.

Teguh Prasetyo, 2013, *Hukum Pidana*, Jakarta : PT. RajaGrafindo Persada.

Wahyudi Djafar dan Asep Komarudin, 2014, Perlindungan Hak Atas Privasi di Internet-Beberapa Penjelasan Kunci. Jakarta: Elsam

C. Regulation

Undang -Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.

Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.

Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PPPSTE).

Peraturan Presiden Nomor 26 Tahun 2009 sebagaimana telah beberapa kali diubah, terakhir dengan Peraturan Presiden Nomor 126 Tahun 2012 tentang Perubahan Ketiga atas Peraturan Presiden Nomor 26 Tahun 2009 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional (Perpres KTP).

Naskah Akademik Undang-undang Perlindungan Data Pribadi, 2022

D. Internet

Australian Press Council, 2014, "Statement of General Principles: Standards' (Statement of General Principles)", *https://www.presscouncil.org.au/uploads/%0A52321/ufiles/GENERAL_-_PRIVACY_PRINCIPLES_-_July_2014*. Diakses pada tanggal 29 September 2023

APWG Phishing Activity Trends Report, 2022, "Phishing Activity Trends Report, 4th Quarter 2022*", https://apwg.org*. Diakses pada tanggal 28 Agustus 2023

Chandra, Mayank & Quraishi, Suhail, 2019, "Phishing Website Classification using Least Square Twin Support Vector Machine*",* *https://www.djkn.kemenkeu.go.id /kpknl-purwakarta/baca-artikel/14851/Waspada-Kehajatan-Phising-Mengintai-Anda.html*, diakses pada tanggal 27 Agustus 2023

CNN Indonesia, 2022, "RI Dihantam 700 Juta Serangan Siber di 2022, Modus Pemerasan Dominan", *https://www.cnnindonesia.com/teknologi*, diakses pada 27 Agustus 2023.

D. Rachmawati, 2020, "Phising sebagai salah satu bentuk ancaman dalam dunia cyber", *http://www.it-artikel.com/*, diakses 18 Desember 2023.

Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri, 2019, "Phising : Apakah Anda Salah Satu Korbannya?", *https://www.patrolisiber.id/*, diakses pada 27 Agustus 2023.

Ensign rilis laporan soroti tren ancaman siber di Indonesia, 2023, *https://www.antaranews.com/berita/3664086/ensign-rilis-laporan-soroti-tren-ancaman-siber-di-indonesia*, diakses pada 27 Agustus 2023.

Guidelines 07/2020, "on the Concepts of controller and processor in the RDPR Verion 2.1",*http://edpb.europa.eu/system/files/202107/eppb_guidelines_202007_controllerprocessor_final_en.pdf*, diakses pada tanggal 29 September 2023.

Jonathan Patrick, 2022, "Ahli: Big Data Jadi Komoditas Utama di Era Digital Indonesia", *https://www.cnnindonesia.com*, diakses pada 24 September 2023.

Mark F. Kightlinger, E. Jason Albert, and Daniel P. Cooper, 1981, "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 28 January", *http://conventions.coe.int/treaty/EN/Treaties/HTML/108.htm*, diakses pada tanggal 5 Oktober 2023

Ni G. A. P. Nitayanti dan Ni M. A. Y. Griadhi, "Perlindungan Hukum terhadap Informasi Pribadi terkait Privacy Right Berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik", *https://ojs.unud.ac.id/index.php/Kerthanegara/article/download/10713/7619*, diakses pada tanggal 5 Oktober 2023.

Paul Voht, "The worlds Biggest data Breaches", *http: //www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/worlds-biggest-data-breaches*, diakses pada tanggal 10 Oktober 2023.

P-ISSN 2723-262X
E-ISSN 2745-9306

Pusiknas Bareskrim Polri, 2023, "Kejahatan Siber di Indonesia Naik Berkali-kali Lipat*",* *https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat*, diakses pada 27 Agustus 2023.

Shilvina Widi, 2023, "Deret Kasus Kebocoran Data RI pada 2023, dari BSI hingga Paspor", *https://dataindonesia.id/internet/detail/deret-kasus-kebocoran-data-ri-pada-2023-dari-bsi-hingga-paspor*, diakses pada 27 Agustus 2023.

Vika Azkiya Dihni, "Jumlah Akun yang Mengalami Kebocoran Data di Indonesia (Kuartal I2020-KuartalII2022)*",* *https://databoks.katadata.co.id/datapublish/ 2022/08/09/kasus-kebocoran-data-di-indonesia-melonjak-143-pada-kuartal-ii-2022*, diakses 23 September 2023.

Z. Ramzan and C. Wuest, 2007, "Phishing Attacks: Analyzing Trends in 2006", *CEAS 2207-4th Conference on Email and Anti-spam, Mountain View,* California USA, *https://www.researchgate.net/publication/220271835_Phishing_Attacks_Analyzing_Trends_in_2006*, diakses pada tanggal 29 Agustus 2025.