Jurnal Hukum
Novelty

Volume 15, Issue 2, 2024, pp. 286-311

P-ISSN: 1412-6834
E-ISSN: 2550-0090

Preventing AI-based phishing crimes across national borders through the reconstruction of personal data protection laws

Gunsu Nurmansyah[1,2]*, I Gede Arya Bagus Wiranata[1], A. Irzal Fardiansyah[1], Stanislav Vladimirov Mladenov[3]

[1] *Lampung University, Indonesia*
[2] *Bandar Lampung University, Indonesia*
[3] *Kazan (Volga Region) Federal University, Russia*

*Corresponding Author: *gunsunurmansyah@gmail.com*

Abstract

Introduction to The Problem: This study focuses on a new form of cybercrime due to advancing technology: AI-based phishing crimes. These crimes involve using artificial intelligence to misuse personal data on digital platforms or applications. Such illicit activities have significant implications and require attention. One significant threat in this context is the rise in AI-based phishing crimes, where attackers use sophisticated AI algorithms to deceive individuals and gain access to their data and information. Establishing solid and comprehensive personal data protection laws is critical to combating AI-based phishing crimes and protecting individuals across national borders.

Purpose/ Study Objectives: The study's object is cross-border AI-based phishing crimes, a new form of cybercrime due to technological advances. This study aims to analyze the concept of personal data protection in Law Number 27 of 2022 from the perspective of substantive justice and the prevention of AI-based phishing crimes.

Design/Methodology/Approach: The author has conducted normative legal research or literature review with a meticulous approach to the principles of criminal law, a comprehensive comparative study of cybercrime law, and an in-depth exploration of the legal history of personal data protection law. Technical analysis, in the form of content analysis, is a series of methods that rigorously analyze the content of all forms of communication, categorizing them into matters related to AI-based cyber phishing, personal data protection regulations, information regulations, and technology.

Findings: Law Number 27 of 2022 on Personal Data Protection can prevent phishing crimes through AI by implementing PDP principles adopted from international PDP principles. This can be done by referring to the OECD Guidelines Governing Privacy Protection and Cross-Border Flow of Personal Data and the data protection regulations in Indonesia.

Paper Type: Research Article

Keywords: Legal Reconstruction; Personal Data Protection; AI-based Phishing Crime; National Borders

Introduction

The rapid advancement of generative AI technology poses a significant threat, potentially exacerbating AI-based phishing crimes. Phishing, a prevalent cybercrime, involves fraudulent attempts to obtain sensitive information. The increase in phishing cases has raised global concerns. Technological progress, particularly in AI, has led to more sophisticated and harder-to-detect phishing techniques. Urgent changes in cybersecurity laws and policies are needed to effectively address these threats. AI enhances the precision and effectiveness of phishing attacks, making them more challenging to identify. Current laws often struggle to keep pace with these technological advancements, hindering law enforcement efforts. More adaptable legislation is necessary to combat the evolving cyber threat landscape caused by AI technology.

Artificial intelligence, a field of computer science, focuses on creating intelligent machines that mimic human functions. It contributes to institutional learning, decision-making, and predictive analytics. Despite promising advancements in financial artificial intelligence, there are significant risks and limitations, including virtual threats, cyber conflicts, changes in human behavior, and legal frameworks needing to catch up with technological developments (Yuspin et al., 2022).

AI research and regulation aim to balance innovation benefits with potential harm. However, the recent surge in AI research has led to potential AI technology misuse for criminal activities, known as AI crime (AIC). AIC is theoretically possible due to experiments in automating fraud and AI-driven market manipulation demonstrations (King et al., 2020). This technology empowers fraudsters to deceive the public more personally and convincingly. For instance, AI chatbots enable fraudsters to craft spear-phishing emails using individual social media posts, while AI-powered voice cloning scams are rising. According to the Trade Regulation Rule on Impersonation of Government and Businesses (2024), scammers exploit voice cloning tools to mimic the voice of a loved one in a difficult situation or a celebrity selling counterfeit goods, thereby spreading fraud more cheaply, precisely, and continuously than ever before. AI-based phishing crimes include impersonation scams involving NFT offerings, mobile apps claiming affiliation with sound recording artists, and phishing scams where a third party claims to be a manager or producer of a music artist. It is unlawful to misrepresent, directly or implicitly, affiliation with, endorsement by, or

Article History
Submitted 5 November 2023 - Revision Required 17 May 2024 - Accepted 21 November 2024

sponsorship from any person for financial gain (Hariyono & Simangunsong, 2023). Phishing crimes, a form of cybercrime, result in significant losses by stealing personal information and data. Therefore, Laws No. 1 of 2024, No. 19 of 2016, and No. 27 of 2022 are crucial for addressing this issue In Indonesia, the Criminal Code generally regulates cyber provisions. However, Indonesian legal regulations adhere to the Lex Specialis derogat legi Generalis principle, which means that specific legislation or legal rules take precedence over general ones. Specifically, cyber law in the banking environment is explicitly regulated by the Law on Information and Electronic Transactions, initially enacted as Number 11 of 2008 and later amended to become Law Number 19 of 2016. Furthermore, Law Number 10 of 1998 amends Law Number 7 of 1992 concerning Banking, and Consumer Protection Law Number 8 of 1999 is also relevant. These laws provide legal protection for consumers, which can help individuals feel more secure if their data is misused (Hariyono & Simangunsong, 2023). Today's technological developments have positively affected human civilization's progress. However, technology is also a double-edged sword, as it can trigger unlawful acts in cyberspace, such as cybercrime (Riskawati, 2016).

While the Criminal Code generally regulates cyber provisions, Indonesian legal regulations follow the *Lex Specialis derogate legi Generalis* principle, which means specific legislation or legal rules override general ones. In Indonesia, a law explicitly regulates cyber law in the banking environment, namely the Law on Information and Electronic Transactions Number 11 of 2008, amended to become Law Number 19 of 2016. Additionally, Law Number 10 of 1998 amends Law Number 7 of 1992 concerning Banking and Consumer Protection Law Number 8 of 1999. With legal protection for consumers, individuals will feel more secure if their data is misused (Ekayani, 2023).

IDADX's phishing activity trend report analyzes phishing attacks and other identity thefts on .id domain names. This report is obtained from the results of APWG data reported by its members at http://www.apwg.org. The number of phishing reports received by IDADX in the first quarter of 2023 reflects a significant increase. In Q1 2023, there were 26,675 phishing reports, compared to 6,106 in Q4 2022, showing a rise of 20,569 reports. Based on these reports, 26,464 were phishing data incidents. The industry sector most targeted for phishing attacks is social media at 45%, followed by the financial institution sector at 31%. This is a change from previous quarters, where financial institutions were the most targeted. However, the social media sector saw a 38% increase in phishing attacks from Q4 2022 to Q1 2023 (Indonesia Anti Phishing Data Exchange, 2023). This data indicates that Indonesia still needs more vigorous law enforcement and protection for the community, especially for victims of cyber crimes like phishing.

Cybercrime phishing involves criminal activities using internet technology to attack public and private facilities. These acts exploit computer and telecommunications technology and can occur anywhere, even across countries. Perpetrators, known as hackers, possess programming skills acquired through various means. Legal protection is provided by the ITE Law and the Personal Data Protection Law in Indonesia to reduce cybercrimes. Cybercrime involves using advanced computer skills to create malware and exploit weaknesses in computer systems and networks (Tarafdar & Fay, 2018). The use of "Cyber" for crimes committed by parties with high abilities and expertise in computer science. Cybercrime is an agreement about computer mastery and computer programming to create malware scripts/codes, and they can analyze how computer systems and networks work, find solutions for the system, and then use those weaknesses to take preventive measures such as storage (Setiawan, 2020).

Cyber phishing crimes involve illegal activities carried out using the internet, often including hacking, stealing personal information, and creating fake credit cards. Perpetrators, known as hackers, acquire their skills through various means. These crimes are driven by technical and economic motivations and are regulated by the ITE Law and the Personal Data Protection Law (Hariyono, 2022). The Data Protection Act (DPA) 1998 establishes the legal framework for handling personal information, also known as 'data subjects.' The Act governs information 'processing,' covering its acquisition, storage, consultation, dissemination, and deletion (Tarafdar & Fay, 2018).

Protecting personal data is considered urgent as part of human rights, regulated by Article 12 of the Universal Declaration of Human Rights (UDHR). This article provides a legal basis for member states' obligations to protect and respect their citizens' rights to privacy. The International Covenant on Civil and Political Rights (ICCPR) also enforces these protections (Situmeang, 2021). The Law on Personal Data Protection in Indonesia, mandated by Article 28G, paragraph (1) of the Constitution, comprises 18 chapters and 76 articles. It regulates the transfer of personal data, administrative procedures, institutional roles, international cooperation, community participation, dispute resolution, procedural law, prohibitions on using personal data, criminal provisions, and transitional and closing provisions. These regulations are detailed in Law Number 19 of 2016, which amends Law Number 11 of 2008 concerning Information and Electronic Transactions under Article 26, specifying that electronic information containing personal data may only be used with the person's permission (Jonimandala, 2023).

The right to privacy is crucial, but safeguarding it in a rapidly changing technological landscape is increasingly challenging. Data processing advancements enable the rapid transmission of vast amounts of data across borders, emphasizing the importance of protecting personal data. Article 28G, Paragraph (1) of the Republic of Indonesia Constitution of 1945 (UUDRI 1945) governs privacy rights in Indonesia, affirming citizens' entitlement to protect themselves, their families, honor, dignity, and property. Most developed countries have established basic data protection legislation (Muir & Oppenheim, 2002).

Article History
Submitted 5 November 2023 - Revision Required 17 May 2024 - Accepted 21 November 2024

The legislation related to e-commerce, electronic publishing, privacy, and security often involves conflicting interests. Governments aim to support these industries while safeguarding individuals' rights and addressing privacy concerns. At the same time, they also seek to protect the government, citizens, and property from terrorist threats. As a result, the legislation may sometimes appear contradictory, offering certain protections while diluting or failing to implement them altogether. It will take time to determine whether governments can achieve a balanced approach (Muir & Oppenheim, 2002). Also, the POJK Consumer Protection Number 1/POJK.07/2013 addresses Consumer Protection in the Financial Services Sector. As for the points in POJK Number 77/POJK.01/2016, it also generally regulates consumer protection:

1. Article 24, Explanation that a Virtual Account is a technology-based service providing facilities for borrowers.
2. Article 29 explains that all lending and borrowing activities must be fair, transparent, open, and without conflict resulting in unilateral harm.
3. Article 30 - 32, In lending and borrowing transactions, all must be easily understood using polite Indonesian accepted by all groups. The explanation is transparent, without any words that are difficult to understand.
4. Article 34, In the service, the criteria given must follow the portion of the candidate bids.
5. Article 35 products must have a license supervised by OJK.
6. Article 36, the lender must provide a clear and standard agreement based on the established law.
7. Article 38 An operational activity already has Pindar standards, has a permit from the OJK, and complies with applicable laws, starting from transaction activities and grouping electronic documents.
8. Article 40, organizers accommodate user complaints and must make periodic reports to the Customer submitting a response or report. It must be prepared periodically and regularly and forwarded to the OJK.

The challenge of addressing cybercrime extends beyond the formulation of criminal law policies to include the harmonization of policies across nations, as cybercrime has evolved into a global issue transcending national boundaries (Purwaningsih & Putranto, 2023). Cyberattacks, often orchestrated by states, are calculated attempts to infiltrate another nation's computer systems or networks, aiming to inflict damage or disruption. Foreign intelligence agencies frequently leverage cyber technologies to conduct espionage and acquire sensitive intelligence. Globally, numerous incidents underscore the devastating misuse and compromise of a nation's information infrastructure, encompassing computer systems, internet networks, and embedded processors and controllers critical to various industries (Masyhar & Emovwodo, 2023).

The Indonesian government is enhancing personal data protection laws to address the rising threat of AI-driven phishing crimes, aiming to safeguard individuals globally. With the rapid advancement of technology, cybercrime—particularly phishing schemes exploiting personal data through AI—has become a pressing concern. This paper focuses on analyzing the personal data protection framework established by Law No. 27 of 2022, with the aim of addressing and preventing AI-driven phishing crimes within the scope of this legislation.

Methodology

The author adopts a Doctrinal Approach (Legal Doctrine Approach), which entails a comprehensive examination of extant legal texts, statutes, regulations, and judicial precedents. This study will critically analyze relevant legal instruments, including data protection statutes, cybersecurity regulations, and policies governing AI applications for phishing detection and prevention. Through this approach, the research aims to identify gaps or ambiguities within current data protection frameworks and AI-related cybersecurity laws. Such an analysis illuminates how existing legislation may fall short in addressing the complexities and challenges associated with AI technology, especially in relation to phishing and data privacy concerns. The study also integrates a normative juridical approach and a qualitative descriptive methodology for data analysis. It primarily focuses on legal norms and regulatory frameworks, employing statutory interpretation and a literature review as core research methods. By means of qualitative inquiry, the study seeks to explore legal norms and regulations both conceptually and in statutory terms. A rigorous technical analysis will examine the content of various communications, categorizing them into themes related to AI-driven cyber phishing, personal data protection laws, information governance, and technology.

Furthermore, the study will evaluate the practical implications of the proposed legal standards. This entails assessing the applicability of the law in real-world legal cases, the effectiveness of regulations in enforcement practices, and their impact on personal data security and AI-powered phishing prevention. This approach serves as a foundation for the development of a legal framework capable of adapting to and addressing the challenges presented by AI technology, while ensuring the protection of personal data in the contemporary digital landscape.

Results and Discussion

Analysis of the Concept of Personal Data Protection in Law Number 27 of 2022 concerning Personal Data Protection from the Perspective of Substantive Justice

The issue of personal data protection, as addressed in Law Number 27 of 2022, represents a critical legal development in the contemporary digital age. With the exponential increase in the collection and processing of personal data across various sectors, the establishment of robust legal safeguards is imperative to protect individual privacy and prevent misuse. This legislation provides a comprehensive framework regulating the collection, use, and disclosure of personal data while affirming individuals' rights to access, rectify, and delete their information stored by others.

The Academic Paper underpinning Law Number 27 of 2022 underscores the intrinsic link between personal data protection and the right to privacy, highlighting its role in safeguarding personal integrity and dignity. This perspective aligns with Indonesia's legal traditions and reflects the pressures of aligning national standards with those of international economic partners (Komarudin, 2014). Thus, the law is both a response to domestic imperatives and a strategy to maintain global competitiveness and compliance.

Historically, the concept of privacy has deep roots in Indonesian legal systems. The earliest known regulation addressing privacy was the Staatsblad King Decree No. 36 of 1893, which authorized the interception and confiscation of letters and other communications in post offices across Indonesia (Yuniarti & Rosadi, 2023). This historical precedent illustrates the longstanding concern with balancing state authority and individual rights, a theme that continues to influence modern legislation.

Indonesia's legal framework for privacy and data protection is remarkably comprehensive. Article 28G of the 1945 Constitution serves as a constitutional mandate for developing laws that safeguard personal data. The Telecommunications Law explicitly prohibits unauthorized wiretapping, protecting the confidentiality of telecommunication transmissions. Additional regulations, such as Law No. 23 of 2006, Law No. 24 of 2013, and Law No. 14 of 2008, prohibit the unauthorized disclosure of personal data and reinforce privacy as a fundamental citizen's right. Yuniarti (2019) identified at least 30 legal instruments across Indonesia's legal system that address personal data protection, indicating the depth and breadth of this issue.

Moreover, international legal norms, such as Article 12 of the Universal Declaration of Human Rights (1948), provide a global benchmark, emphasizing the right to privacy and protection from arbitrary interference. Personal data protection is increasingly understood as a cornerstone of respecting individual autonomy and dignity. Beyond its ethical dimensions, personal data holds significant economic value (Makarim, 2004), necessitating legal structures that balance individual rights with the demands of a data-driven economy. Thus, Law Number 27 of 2022 is not merely a regulatory response but a crucial component of Indonesia's broader commitment to protecting privacy, adapting to global legal trends, and ensuring the economic and social integrity of its citizens in an era defined by data.

The academic commentary on the legislative framework governing Law Number 27 of 2022 on Personal Data Protection offers a comprehensive analysis of the terminology and provisions outlined in the statute, thereby providing essential clarity and regulatory direction. In order to fulfill its constitutional duty to safeguard the fundamental rights of its citizens, the State must implement various protective mechanisms as prescribed by the Law. These mechanisms are encapsulated in the following key obligations:

1. Safeguarding Individual Privacy: a. Instituting comprehensive regulations governing the collection, processing, and dissemination of personal data. b. Affirming the individual's right to access, correct, and delete personal data held by third parties.
2. Preventing the Misuse of Personal Data: The Law mandates the establishment of robust safeguards to prevent the exploitation or inappropriate use of personal data.
3. Ensuring Substantive Justice and Protection of Fundamental Rights: The overarching goal of the Law is to maintain substantive justice by ensuring that individuals' fundamental rights, particularly their privacy and autonomy, are consistently protected against infringement.

This structure reinforces the State's duty not only to regulate the handling of personal data but also to ensure that such regulation translates into concrete protections for citizens, maintaining a balance between the effective use of personal data and the preservation of individuals' rights.

These aspects are elaborated upon by the author as follows:

1. Protecting individual privacy

   Data protection regulations, recognized internationally as essential for safeguarding individual privacy, encompass fundamental human rights and rights to private property. These protections are vital amidst technological advancements and organizational developments, public concerns surrounding these advancements, and other legal frameworks that provide normative bases for regulation (Tan, 2008; Weber, 2010). Human rights are difficult to define and can vary across contexts and cultures. Privacy aims to protect personal space and can be categorized into information, bodily, communications, and territorial privacy (Makarim, 2004).

   According to Alan Westin's theory, privacy and data protection involve individuals, groups, or institutions asserting their right to determine when, how, and to what extent information about them is communicated to others. Privacy encompasses personal autonomy, emotional well-being, self-evaluation, and controlled and protected communication (Westin, 1967). Regulating personal data collection, use, and disclosure is crucial for safeguarding individuals' privacy and security. It is essential to ensure that personal data is collected and used only for legitimate purposes, with explicit consent from the individual, and protected against unauthorized access or misuse. Effective regulations are essential in today's digital era to uphold the privacy and security of personal data.

2. Personal data

   There is a significant discrepancy between the definition of personal data concerning a specific individual and the socio-technical context in which it is used. For instance, the current model cannot represent scenarios where multiple people

Article History
Submitted 5 November 2023 - Revision Required 17 May 2024 - Accepted 21 November 2024

use the same device. These services cannot verify which user accessed the device, leaving room for potential data privacy breaches, as one user may gain access to data that another user had intentionally deleted (Urban et al., 2018). As per Law Number 14 of 2008 on Public Information Openness, information includes statements, ideas, signs, data, facts, and explanations presented in various formats, continuously evolving with technological advances.

3. Sensitive personal data
   In today's digital age, sharing information online is essential for staying connected. However, it's important to be mindful of the risks of sharing too much personal information, which can lead to data leaks. Online social network providers use various technical methods to protect users' privacy, such as access control, cryptography, and privacy-preserving data processing (Dang et al., 2020).

According to the UK Data Protection Act 1998, sensitive personal data is personal data consisting of information regarding:

1. The race or ethnic origin of the data owner;
2. Political views;
3. Religious beliefs or other beliefs of a similar nature;
4. Membership in trade unions;
5. Physical state or mental health;
6. Sexual life;
7. Violation or suspicion of a breach committed;
8. Information on the trial of the offense or alleged violation committed by him and the decision taken by the court for the breach;
9. Information about the trial for the offense or alleged violation committed by him, including the decision made by the court regarding the breach;

The right of individuals to access, correct, and delete their personal data is fundamental to ensuring control over one's personal information, protecting privacy, and preventing potential misuse of data by organizations. Indonesia's national legislation incorporates Personal Data Protection (PDP) principles that are closely modeled after international frameworks. Specifically, Indonesia's data protection laws, both prior to and following the enactment of the PDP Law, are in harmony with the OECD Guidelines on Privacy Protection and the Cross-Border Flow of Personal Data. This alignment underscores the country's commitment to adhering to internationally recognized data protection standards. As such, the principles embedded in Indonesian data protection laws are in precise conformity with the global PDP norms, including those established by the OECD, both before and after the PDP Law was introduced. Additionally, Indonesia's regulatory approach to data protection reflects a broader trend in Asia toward aligning with international data protection frameworks (Yuniarti, 2019).

The analysis of privacy and data protection is inherently intertwined with the broader framework of human rights. In Indonesia, the protection of personal data spans multiple areas of law, notably human rights law and telecommunications law. However, the practical enforcement of privacy and data protection within the country is often constrained by considerations of public interest. This necessitates a delicate balance, ensuring that individual privacy rights are not upheld at the expense of other fundamental rights, while also accounting for prevailing societal norms, cultural values, and religious principles (Palupy, 2011).

Gustav Radbruch's theory of substantive justice underscores the imperative of striking a balance between legal certainty, the lived experiences of legal actors, and the pursuit of justice in its truest sense. His framework suggests that the law must go beyond mere formalism and account for ethical and moral considerations to achieve genuine fairness. In this context, research has shown that Indonesia's Law Number 27 of 2022 on Personal Data Protection (PDP Law) aligns with these principles of subjective justice. Specifically, the law embraces a more restrained approach to data collection, ensuring that personal data is only gathered when necessary and for legitimate purposes, reflecting a commitment to individual rights while balancing broader social needs.

This law enacts several core principles designed to protect individual rights and ensure that personal data is handled in a just and responsible manner:

1. Principle of Collection Limitation: Data collection must be limited, specific, legally justified, and transparent.
2. Principle of Data Quality: The data must be accurate, complete, non-deceptive, current, and accountable for its usage.
3. Principle of Purpose Limitation: Data processing should be aligned with the purpose for which it was collected; once the retention period expires or upon the data subject's request, the data must be destroyed or deleted, except where law dictates otherwise.
4. Principle of Security Protection: Measures must be in place to protect personal data from unauthorized access, disclosure, alteration, misuse, destruction, and negligence.
5. Principle of Transparency: Data subjects must be notified of the objectives of data processing, the activities involved, and any breaches of data protection.
6. Principle of Individual Participation: Individuals must have the right to access and control their data, and data controllers must be held accountable for their actions in a manner that is verifiable and responsible.

The rapid advancement of technology and the growing forces of globalization have presented significant challenges in safeguarding individual privacy rights. Modern technologies have made personal data more accessible than ever, with both private and public entities extensively utilizing this information. Simultaneously, individuals

Article History
Submitted 5 November 2023 - Revision Required 17 May 2024 - Accepted 21 November 2024

are increasingly willing to share their personal details, making data protection a critical element of legal frameworks in today's information-driven society (Tchinaryan et al., 2019).

In Indonesia, however, the regulation of personal data protection remains insufficient and requires substantial reforms. Key issues include weak regulatory frameworks, inconsistent law enforcement, and the deliberate manipulation of personal data during election processes. A more rigorous approach is necessary to enforce laws protecting personal data. Indonesia can benefit from examining the successful frameworks implemented by the European Union or neighboring countries, which view personal data protection not only as a legal obligation but as an essential component of upholding human rights and justice (Ananthia, 2019).

Organizations, as data controllers or processors, must take proactive steps to prioritize data security, regularly conducting audits to ensure compliance with regulations. They should also seek certifications for reliability and consult with cybersecurity experts to implement tailored cybersecurity measures to meet legal requirements and mitigate risks (Vania et al., 2023). The establishment of the Personal Data Protection Supervisory Agency (BPDP) in Indonesia under Law No. 27 of 2022 is a positive step, as it introduces significant penalties, including imprisonment of up to five years and fines up to IDR 5 billion for the intentional and unlawful misuse of personal data. These penalties are intended to heighten awareness and foster greater compliance among data controllers, ensuring the protection of individuals' personal information in an increasingly digital world (Mahameru et al., 2023).

However, Indonesia's personal data protection laws remain outdated and inadequate. The current regulatory framework offers only partial protection, underscoring the urgent need for a comprehensive overhaul. The implementation of more robust and inclusive regulations would not only safeguard AI applications but also reduce the risk of cybercrimes targeting consumer data. Furthermore, the existing regulations remain sectoral in nature, highlighting the pressing need for a unified, nationwide approach (Sulistianingsih et al., 2023). The evolution of personal data protection law aligns with the convergence theory of law, which provides a framework for understanding how technological, economic, and legal forces interact to shape human and societal relationships in the digital era at the national, regional, and international levels (Danrivanto Budhijanto, 2014). The principles, rules, and institutions embedded in this legal framework reflect the realities of modern life in the Fourth Industrial Revolution, contributing to the emergence of a global digital civilization (Budhijanto, 2023). Upon reviewing the structure of Indonesia's Personal Data Protection Law (No. 27 of 2022), it is evident that the law aims to achieve legal certainty, efficiency, and justice. These objectives are vital for ensuring substantive justice in Indonesia's criminal law system. Upholding substantive justice and protecting individuals' fundamental rights are essential principles, ensuring that all citizens are treated equitably, regardless of their background or circumstances.

Moreover, the concept of subjective justice, as articulated in the Preamble of the Indonesian Constitution, emphasizes human rights as central to the nation's ideals and goals. The Constitution envisions a national mission that encompasses the protection of Indonesian citizens, the promotion of the general welfare, the education of the nation, and the establishment of a global order based on freedom, social justice, and world peace.

AI-based Phishing Crime Prevention in Law Number 27 of 2022 concerning Personal Data Protection

Phishing represents a sophisticated malicious technique employed by cyber attackers to exploit users and obtain sensitive personal information. This represents a significant cybersecurity challenge, as attackers often construct deceptive websites that mimic legitimate ones, aiming to deceive unsuspecting individuals. From a technical perspective, phishing can be understood as a classification problem, where a machine learning model or classifier is developed through the analysis of various website features (Chandra et al., 2019). This criminal activity relies heavily on social engineering tactics, wherein phishers endeavor to fraudulently acquire confidential data, including usernames, passwords, and credit card numbers, by impersonating reputable entities in electronic communications (Mihai, 2012).

Research into phishing has highlighted the role of cognitive vulnerabilities in facilitating victimization. People often fall prey to phishing attacks due to ineffective cognitive processing, which diminishes their ability to critically assess the legitimacy of incoming communications. Consequently, preventive measures have largely focused on enhancing users' skills to identify deceptive emails. However, studies indicate that the effectiveness of such training diminishes over time, as users tend to develop habitual patterns of email interaction that undermine their vigilance against phishing attempts (Vishwanath et al., 2018).

Furthermore, a study indicates that internet users are more prone to clicking on emails related to protecting their assets. However, an overemphasis on fear-based appeals within these communications can lead to a disproportionate response to phishing attempts. Empirical findings demonstrate that users who fixate excessively on fear-inducing language often fail to adequately assess the authenticity of the scenarios presented in email phishing attacks, making them vulnerable to fraudulent attempts. This suggests that while training and awareness campaigns can be beneficial, they must be carefully designed to strike a balance between fear and rational decision-making to be effective (Akdemir & Yenal, 2021).

1. Spear Phishing

   Spear phishing is a type of email phishing with a more targeted approach. Unlike regular phishing, which usually involves random mass email delivery, spear

Article History
Submitted 5 November 2023 - Revision Required 17 May 2024 - Accepted 21 November 2024

phishing is directed at specific individuals or organizations. Attackers typically obtain basic information about their targets, such as their names and addresses, before launching a spear phishing attack.

2. Whaling
   Whaling is a phishing attack that targets individuals who hold high positions in an organization, like business owners, company directors, and personnel managers. If successful, this attack can provide unauthorized access to sensitive information and systems, which can be exploited for various benefits.

3. Web Phishing
   Web phishing attempts to trick potential victims by creating fake websites resembling official ones, often using similar domain names. This practice is called domain spoofing.

OpSec Security, a founding member of APWG, released its Phishing Activity Trends Report for Q4 2022. The report highlights that phishing attacks against the financial sector, including banks, accounted for 27.7% of all phishing attacks, up from 23.2% in the previous quarter. Attacks on webmail and SAAS providers came in next, accounting for 17.7% of all attacks, slightly down from Q3. Attacks on payment processors such as PayPal, Venmo, and VISA accounted for 6% of all phishing attacks (APWG Phishing, 2022).

IDADX's phishing activity trends report analyzes phishing attacks and other identity thefts on .id domain names. IDADX also receives reports from its members through the http://idadx.id website, Google Web Risk, and phishing reports from the public. It is reported that the number of phishing attacks in the last five years is 69,117, and the number of phishing attacks reported in Q1 2023 is 26,675. Organizations most targeted by phishing attacks in Q1 2023 include Facebook, with the social media industry being the primary target. At present, phishing is usually done through social engineering schemes and technical subterfuges. Social engineering targets unwary victims by manipulating them into believing they are dealing with a trusted and legitimate party, such as sending fraudulent messages via email addresses. Subterfuge involves planting malware into computers to steal credential information from victims, usually by intercepting usernames and passwords or redirecting users to fake websites. As a result of these scams, more and more consumers suffer from credit card fraud, identity theft, and financial loss (Indonesia Anti Phishing Data Exchange, 2023).

Phishing attackers consistently devise innovative ways to bypass anti-phishing schemes. Consequently, ongoing demands are essential to generating innovative anti-phishing strategies based on web mining and machine learning (Zuhir, 2015). The classification of phishing is a unique issue in data mining. The objective is to predict whether a website is "legitimate," "phishing," or "suspicious" based on input data sets, known as training data sets. These sets contain information distinguishing website features from the target class (Al-diabat, 2016).

Legal Instruments Against Cybercrime in the Form of Phishing

The legal framework for addressing cybercrime in the form of phishing was previously covered by Article 378 of the Criminal Code, which pertains to fraud. Phishing is generally considered a form of fraud. According to Article 378 of the Criminal Code, fraud is defined as: "Whoever, with the intent to unlawfully benefit themselves or others, uses a false name or false identity, deception, or a series of lies to induce another person to give them something or to forgive a debt or relinquish a claim, shall be guilty of fraud and may be imprisoned for up to four years."

Based on the elements described in Article 378 of the Criminal Code, it can be concluded that "whoever" refers to the perpetrator committing the crime of fraud. There is an intention to benefit oneself or others, meaning an intention done as an "*oogmerk*" (intent). Furthermore, the act is carried out unlawfully, meaning the perpetrator of the fraud has no right at all to enjoy the benefits that result from the fraud (Hamzah, 2015).

Nevertheless, based on the principle of "*Lex Specialis Derogat Legi Generali*," rules of an exceptional nature are considered valid even if they conflict with the general rule of law regulations. It can be concluded that the current legal regulation of cybercrime in the form of phishing is governed by Law Number 1 of 2024, which amends Law Number 19 of 2016, itself an amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.

The crime imposed on cybercrime in the form of phishing is subject to layered articles, namely Article 28 paragraph (1) in conjunction with Article 45A paragraph (1) or Article 35 in conjunction with Article 51 paragraph (1). The punishment must not exceed the maximum of the heaviest crime plus one-third, known as the softened cumulation system this is called "*Concursus Realis*," which occurs when a person commits several acts, each standing alone as a criminal act, and the crimes committed need not be similar or even related to one another (Prasetyo, 2013). Based on the description above, phishing perpetrators who have violated Article 28 paragraph (1), Article 45A paragraph (1), and Article 35 paragraph (1) of Law Number 1 of 2024, which amends Law Number 19 of 2016, itself an amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, will be prosecuted.

Phishing is deemed illegal because it constitutes a criminal offense that causes harm to individuals. Specifically, phishing is categorized as a material offense, as it involves unlawfully obtaining and exploiting personal, confidential information from victims. However, the provisions in Article 35 in conjunction with Article 51, paragraph (1) of the relevant laws do not explicitly address the elements of deceit that inflict harm on others. Similarly, Article 28, paragraph (1) in conjunction with Article 45A, paragraph

Article History
Submitted 5 November 2023 - Revision Required 17 May 2024 - Accepted 21 November 2024

(1) fails to address the manipulation, creation, or alteration of electronic information and documents to ensure their authenticity. Consequently, these articles do not encompass actions such as the creation of fraudulent websites that mimic legitimate official sites. This gap in the legal framework has led to ambiguity in the legal treatment of phishing under Law Number 1 of 2024, which amends Law Number 19 of 2016, and which itself modified Law Number 11 of 2008 on Electronic Information and Transactions (Gulo et al., 2021). The failure of Law Number 19 of 2016, as amended by Law Number 11 of 2008, to explicitly define phishing creates significant challenges in prosecuting cybercrime in the form of phishing, thereby hindering the effective enforcement of laws against such offenses.

Phishing, as broadly defined, is a scalable form of deception in which impersonation is employed to extract sensitive information from a target. The mechanics of phishing are shaped by various fraudulent schemes, such as digital exploitation and widespread communication over networks, which provide perpetrators with novel means to exploit human vulnerabilities on an unprecedented scale (Lastdrager, 2014). In Indonesia, the Personal Data Protection Law (Law No. 27 of 2022) governs the collection, processing, and storage of personal data to safeguard the privacy rights of citizens. The law is enforced by the Personal Data Protection Supervisory Agency (BPDP), ensuring the legal and secure handling of personal data.

The application of personal data in artificial intelligence (AI) systems raises significant concerns regarding human rights and the protection of personal information. Technological advancements in AI have complicated the formulation of effective strategies to ensure data protection, with risks including unauthorized data access, identity theft, and the potential for AI-driven discrimination or fraud. To mitigate these risks, stringent regulations, data encryption, and comprehensive user education are paramount (Clifford et al., 2020). However, the rigor with which personal data is regulated varies across jurisdictions, despite global efforts to achieve legal harmonization. One key difference in existing data protection frameworks lies in whether certain types of data—categorized as 'sensitive' or 'special'—require stricter legal safeguards and operational protections (Bielova & Byelov, 2023). This underscores the challenges posed by the increasing integration of AI into daily life, which can both amplify threats and complicate the enforcement of personal data protection laws.

AI's role in combating phishing includes leveraging machine learning, real-time monitoring, user behavior analysis, and natural language processing to detect and mitigate phishing attacks with greater speed and accuracy. These advanced capabilities highlight AI's potential to offer more robust and effective protection compared to traditional detection methods.

1. AI can detect phishing attacks early and accurately using machine learning to analyze email and message patterns for common characteristics of phishing

attacks, such as specific words, suspicious link patterns, and unusual sender domain settings. This helps identify threats before they reach their targets (Sahingoz et al., 2019).
2. AI can monitor real-time user activity to detect anomalies or suspicious behavior that may signal a phishing attempt. AI-based systems, such as deep learning, can adjust their algorithms based on the latest data, allowing for a more adaptive response to ongoing threats. This can include automating responses to potential attacks, such as blocking suspicious emails or locking out accounts that have been indicated to have been exposed to phishing attacks (Gupta et al., 2017).
3. AI also utilizes user behavior analysis to detect unusual or suspicious patterns that may indicate a phishing attempt. By studying user habits such as typing, location, or access time, AI can detect anomalies indicating a user's account has been compromised or is targeted for an attack. This approach aids in the identification and prevention of increasingly sophisticated and complex attacks (Xun Dong et al., 2008).
4. AI uses Natural Language Processing (NLP) techniques to analyze the language used in phishing emails or messages. NLP techniques help detect manipulative signs in language, such as false urgency or sentences designed to deceive the recipient. With this capability, AI can identify phishing more accurately, even when the attack uses never-before-seen tactics (Aggarwal et al., 2012).

Artificial intelligence presents a promising approach to combating phishing attacks through advanced techniques such as automated detection, behavioral analytics, and real-time monitoring. Leveraging machine learning and deep learning algorithms, AI can identify patterns indicative of phishing attempts, even in the context of large and complex datasets. However, the practical implementation of AI for this purpose is subject to several significant limitations.

1. The Necessity for Extensive and High-Quality Data for Algorithm Training: AI systems require vast quantities of high-quality data to effectively train their algorithms for phishing detection. Inadequate or insufficient data hampers the ability of AI to detect novel or sophisticated phishing methods, ultimately compromising its adaptability and reducing its overall effectiveness (Gupta et al., 2017). Without continuous access to diverse, comprehensive datasets, AI systems may struggle to keep pace with evolving phishing techniques, limiting their capacity for proactive defense.
2. Challenges with False Positives: While AI-driven cyber threat detection systems can enhance the accuracy of identifying phishing attempts, they are not immune to the issue of false positives. The use of event profiles in AI systems can reduce the frequency of such errors, yet false positives remain a significant challenge, often necessitating human intervention to distinguish legitimate threats from benign activities (Lee et al., 2019). These false alarms, if not properly managed, can undermine user confidence in AI-driven security measures.

Although AI has the potential to significantly enhance the detection and prevention of phishing attacks, it faces notable practical constraints. These include the need for substantial and high-quality data for training algorithms, the challenges posed by false positives, and the constant requirement for updates to stay ahead of evolving phishing tactics. Furthermore, high false positive rates can diminish user trust in AI systems. To maximize AI's effectiveness in this domain, a comprehensive approach is necessary. This should combine technological advancements with a robust set of data protection policies, including stricter regulations surrounding data collection and processing, as well as increased transparency in AI algorithms. Such measures would not only improve the accuracy of phishing detection but also ensure that users are better informed and empowered to resolve errors promptly.

AI systems demonstrate the potential to detect and mitigate phishing attempts, but they are constrained by several practical limitations. Training algorithms to effectively identify phishing requires vast datasets and continuous updates to keep pace with rapidly evolving tactics, demanding significant resources. Furthermore, the risk of high false positive rates may undermine user confidence in these systems, as legitimate communications might be flagged as fraudulent. To address these challenges, a holistic strategy is essential—one that integrates technological innovation with tailored data protection frameworks. This strategy should incorporate stringent regulations surrounding data collection and processing, alongside efforts to enhance algorithmic transparency, thereby fostering greater user awareness and facilitating more effective error resolution.

First, the issue of Data Protection and Privacy must be examined. AI's reliance on large datasets to train algorithms and make predictions often intersects with existing data protection laws, such as the European General Data Protection Regulation (GDPR), which governs the collection, storage, and use of personal data. AI-driven practices can risk breaching these regulations, particularly when personal data is used without explicit consent or for purposes not previously disclosed. There is also the issue of excessive data usage, which contravenes data minimization principles enshrined in many data protection regulations (Meurisch & Mühlhäuser, 2022). These concerns necessitate a careful balance between leveraging data for AI advancements and ensuring the protection of individuals' privacy rights.

Second, ensuring Transparency and Accountability in AI systems is an ongoing challenge. The "black box" nature of many AI algorithms—the lack of visibility into their decision-making processes—creates significant hurdles in holding systems accountable for their actions. This opacity complicates the identification of responsibility when errors or harmful outcomes occur, such as discriminatory or unjust decisions made by AI. Determining legal liability in such cases can be complicated, as it may involve multiple stakeholders, including software developers, data providers, and the end-users of AI technologies. Without clearer insights into how AI systems operate and make decisions, assigning accountability for adverse effects remains a complex and unresolved issue (Kardos, 2022).

Third, AI technology holds significant potential for applications that could undermine both public and private security. AI algorithms, for example, could be manipulated to facilitate increasingly sophisticated cyberattacks or generate deepfakes that are difficult to detect, presenting substantial risks. These developments introduce novel legal challenges, underscoring the urgent need for more robust regulatory frameworks to govern the use of AI and mitigate potential misuse. Current legal structures may need to be revised to impose more severe penalties for harmful AI applications and ensure that AI systems are developed with enhanced security protocols to prevent such threats (Rangaraju, 2023).

In this context, existing regulations such as the General Data Protection Regulation (GDPR) may require significant updates to account for the evolving capabilities of AI technologies. These updates might include clarifying the rights of data subjects, establishing transparency standards for AI-driven decision-making processes, and creating comprehensive guidelines for the secure, ethical development and deployment of AI systems. Additionally, clear accountability mechanisms must be instituted to address potential errors or harmful consequences arising from AI misuse. The development and implementation of AI-powered systems demand considerable investments in technical resources and ongoing governmental support, as well as cooperation from various stakeholders. The European Union (EU) serves as an instructive model of governmental backing for AI advancements. However, the regulatory framework being introduced in the EU will impose significant financial burdens on organizations, especially given the scale and complexity of the implementation process (Colmenarejo et al., 2022).

Furthermore, AI startups face substantial compliance costs as they navigate the increasingly complex landscape of international regulations, which disproportionately impacts smaller entities compared to larger, more resource-rich tech companies with established infrastructures (Wu & Liu, 2023). Attention should also be given to the U.S. government's substantial investments in AI initiatives. While significant funds have been allocated to these efforts, challenges persist in ensuring their effective deployment and in maximizing the potential benefits of these investments (Selyanin, 2021).

The use of AI to monitor and analyze behavioral patterns inevitably raises significant concerns regarding privacy and ethics. To mitigate these risks, robust safeguards must be implemented to protect individual privacy. Emerging technologies such as differential privacy, homomorphic encryption, and federated learning provide secure means of processing personal data while preserving the confidentiality of sensitive information (Petar Radanliev & Omar Santos, 2023). However, to address the evolving and multifaceted risks associated with AI, more stringent and precise regulations are required. Specifically, there is a need to limit the use of personal data in training AI algorithms and to empower individuals with the right to comprehend and control how their data is utilized by AI systems (Tripathi & Mubarak, 2020). Privacy by Design is a crucial framework that incorporates privacy considerations from the very inception of AI systems, which can effectively reduce the likelihood of privacy breaches. This approach involves implementing comprehensive auditing mechanisms, promoting transparency in algorithms, and establishing risk management protocols to ensure compliance with rigorous privacy standards (Pagallo, 2011). Furthermore, new legal rights are necessary to shield individuals from invasive or high-risk data processing activities that may compromise their privacy or damage their reputation. This could include requirements for data controllers to justify the use of personal data in AI-driven inferences (Wachter & Mittelstadt, 2018). To achieve a balanced approach, governments and regulatory bodies must craft policies that both protect privacy and foster technological innovation. This includes developing a clear and adaptive framework for data protection that allows for AI progress while simultaneously upholding individual rights (Carmody et al., 2021). Such measures are essential for creating an ethical and privacy-respecting AI landscape.

Several case studies and specialized research demonstrate the success of AI-powered solutions in preventing phishing attacks. These studies show that AI-based solutions have proven effective in detecting and preventing phishing attacks using machine learning and data analysis techniques:

1. PhishHaven An Efficient Real-Time AI Phishing URL Detection System. The study introduced PhishHaven, a real-time phishing URL detection system that uses machine learning techniques to identify phishing URLs created by humans or AI. PhishHaven can accurately classify URLs with 98% accuracy by employing lexical analysis and HTML URL encoding. Additionally, the system uses a multi-threading approach to improve detection speed, demonstrating its ability to identify future AI-based phishing attacks with 100% accuracy for specific URL types (Sameen et al., 2020);
2. AI antiPhish Machine Learning Mechanisms for Cyber Phishing Attack. The research introduces a machine learning framework for anti-phishing services, incorporating algorithms like Support Vector Machine (SVM), Logistic Regression, and Decision Tree. The study found that the XGBoost model outperformed others, achieving 99.2% accuracy in detecting phishing attacks. These results showcase the efficacy of AI-based solutions in addressing phishing attacks (Chen & Chen, 2019).
3. Prevention of Phishing Attacks Using AI Algorithm. This study introduces an LSTM (Long Short-Term Memory) -based model designed to identify and thwart phishing attacks. The model employs an intelligent AI-driven method to detect phishing websites, particularly emphasizing utilizing the URL feature. Studies

indicate that this model effectively detects phishing attacks and offers enhanced protection for users against cyber threats (Ansari et al., 2022)

4. Detection of Phishing Websites using an Efficient Feature-Based Machine Learning Framework. In the study, a feature-based classification model is introduced, utilizing the Random Forest (RF) algorithm to achieve a 99.31% accuracy rate in detecting phishing websites. Through the analysis of URL features and website source code, this model effectively addresses the limitations of prior anti-phishing methods, demonstrating its ability to detect phishing attacks, including previously unknown ones (Rao & Pais, 2019).

The government has the potential to leverage legal frameworks to bolster its efforts in combating phishing through AI-driven solutions. Artificial intelligence can play a pivotal role in real-time surveillance and analysis of internet users' behavior, enabling the identification of anomalous activities that may signify phishing attempts. Through continuous learning from historical phishing incidents, AI systems can also enhance early detection capabilities, allowing for the swift recognition of emerging threats. However, the deployment of AI in phishing prevention must be carefully calibrated to ensure robust safeguards for personal data privacy. While AI's capacity to analyze patterns and predict phishing attacks is a powerful tool, its use must be governed by stringent data protection principles to prevent misuse or violations of privacy.

In this context, the implementation of Law Number 27 of 2022 offers a legal foundation for integrating AI into phishing prevention measures. By aligning with international data protection standards, such as the OECD Guidelines on Privacy Protection and the Cross-Border Flow of Personal Data, the government can ensure a balanced approach to innovation and privacy protection. Furthermore, adherence to Indonesia’s own data protection regulations is crucial to ensure full legal compliance and the safeguarding of citizens' personal information in the digital age. In sum, while AI presents an invaluable resource for combating phishing, its deployment must be carefully regulated to uphold privacy and data security, ensuring that technological advancements do not come at the cost of individuals' fundamental rights.

Conclusion

The analysis of personal data protection within Law Number 27 of 2022 concerning Personal Data Protection, when viewed through the lens of substantive justice, reveals a strong alignment with the ideals of subjective justice as enshrined in the Preamble of the Indonesian Constitution. This preamble emphasizes the protection of human rights as fundamental to the nation’s ethos and overarching goals. Law No. 27 of 2022 adheres to these principles of subjective justice, notably by integrating key international standards such as the OECD's guiding principles, including the core principle of limiting data collection.

Furthermore, the implementation of this law plays a crucial role in addressing emerging cyber threats, particularly phishing crimes facilitated by artificial intelligence (AI). AI can be both a threat and a solution; while it has the potential to enable more sophisticated cybercrimes, it also offers powerful tools for enhancing data protection. AI technologies, when used responsibly, can help detect and prevent phishing attacks by analyzing patterns, monitoring suspicious activities, and ensuring compliance with data protection principles. By aligning with international standards, including the OECD Guidelines on Privacy Protection and the Cross-Border Flow of Personal Data, Indonesia can leverage AI not only to combat these emerging risks but also to improve the enforcement of personal data protection laws.

Thus, the adherence to Indonesia's data protection framework, complemented by the strategic use of AI, is essential not only for ensuring legal compliance but also for proactively safeguarding personal data in an increasingly interconnected and technologically advanced global environment.

Acknowledgment

This research is part of the author's doctoral program at the University of Lampung.

Declarations

Author contribution	: Author 1 initiated the research ideas, constructed the instruments, collected and analyzed data, and drafted the manuscript; Author 2 revised the research ideas and literature review. Author 3 contributed to data presentation, analysis, and the final draft. Author 4 provided critical feedback and helped shape the research, analysis, and manuscript.
Funding statement	: This research is funded under Universitas Bandar Lampung
Conflict of interest	: The authors declare no conflict of interest.
Additional information	: No further information is available for this paper.

References

Aggarwal, A., Rajadesingan, A., & Kumaraguru, P. (2012). PhishAri: Automatic realtime phishing detection on Twitter. *2012 ECrime Researchers Summit*, 1–12. https://doi.org/10.1109/eCrime.2012.6489521

Akbar Galih Hariyono. (2022). Perlindungan hukum korban pencurian data pribadi (phishing cybercrime) dalam perspektif kriminologi. *Bureaucracy Journal : Indonesia Journal of Law and Social-Political Governance*, *3*(1), 428–439. https://doi.org/10.53363/bureau.v3i1.191.

Akdemir, N., & Yenal, S. (2021). How phishers exploit the coronavirus pandemic: A content analysis of COVID-19 Themed Phishing Emails. *SAGE Open*, *11*(3). https://doi.org/10.1177/21582440211031879

Alan F. Westin. (1967). Privacy and freedom. 25 Wash. & Lee L. Rev. 166. Available at: https*://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20.*

Ananthia. (2019). Perlindungan hak privasi atas data diri di era ekonomi digital. Hasil Penelitian, Pusat Penelitian Dan Pengkajian Perkara, Dan Pengelolaan Perpustakaan Kepaniteraan Dan Sekretariat Jenderal Mahkamah Konstitusi, Jakarta

Andi Hamzah. (2015). *Delik-delik tertentu (speciale delicten) didalam KUHP edisi kedua*. Sinar Grafika.

Ansari, M. F., Panigrahi, A., Jakka, G., Pati, A., & Bhattacharya, K. (2022). Prevention of phishing attacks using AI algorithm. *2022 2nd Odisha International Conference on Electrical Power Engineering, Communication and Computing Technology (ODICON)*, 1–5. https://doi.org/10.1109/ODICON54453.2022.10010185

APWG Phishing. (2022). *Phishing activity trends report, 4th Quarter 2022*.

Bielova, M., & Byelov, D. (2023). Challenges and threats of personal data protection in working with artificial intelligence. *Uzhhorod National University Herald. Series: Law*, *2*(79), 17–22. https://doi.org/10.24144/2307-3322.2023.79.2.2

Bringas Colmenarejo, A., Nannini, L., Rieger, A., Scott, K. M., Zhao, X., Patro, G. K., Kasneci, G., & Kinder-Kurlanda, K. (2022). Fairness in agreement with European Values. *Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society*, 107–118. https://doi.org/10.1145/3514094.3534158

Carmody, J., Shringarpure, S., & Van de Venter, G. (2021). AI and privacy concerns: A smart meter case study. *Journal of Information, Communication and Ethics in Society*, *19*(4), 492–505. https://doi.org/10.1108/JICES-04-2021-0042

Chandra, M. A., Bedi, S. S., Chandra, S., & Quraishi, S. J. (2019). Phishing website classification using least square twin support vector machine. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 2063–2068. https://doi.org/10.35940/ijitee.A3905.119119

Chen, Y.-H., & Chen, J.-L. (2019). AI@ntiPhish — machine learning mechanisms for cyber-phishing attack. *IEICE Transactions on Information and Systems*, *E102.D*(5), 878–887. https://doi.org/10.1587/transinf.2018NTI0001

Clifford, D., Richardson, M., & Witzleb, N. (2020). Artificial intelligence and sensitive inferences: New challenges for data protection laws. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3754037

Dang, T. T., Dang, K. T., & Küng, J. (2020). Interaction and visualization design for user privacy interface on online social networks. *SN Computer Science*, *1*(5), 1–12. https://doi.org/10.1007/s42979-020-00314-9

Danrivanto Budhijanto. (2014). *Teori hukum konvergensi*. Refika Aditama.

Danrivanto Budhijanto. (2023). *Hukum perlindungan data pribadi di Indonesia Cyberlaw dan Cybersecurity)*. PT. Refika Aditama.

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber crime dalam bentuk phising berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law*, *1*(2), 68-81. https://doi.org/10.22437/pampas.v1i2.9574

Article History
Submitted 5 November 2023 - Revision Required 17 May 2024 - Accepted 21 November 2024

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*(12), 3629–3654. https://doi.org/10.1007/s00521-016-2275-y

GW Jonimandala, D. S. (2023). Peran direktorat tindak pidana siber (DITTIPIDSIBER) bareskim polri dalam melakukan penegakan hukum terhadap kejahatan pencurian dan penyalahgunaan data pribadi. *innovative: Journal Of Social Science Research* , *3*(4), 680–692. https://doi.org/10.31004/innovative.v3i4.2874.

H. Zuhir, A. S. and M. S. (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*, *6*(10). 10.14569/IJACSA.2015.061031.

Hariyono, A. G., & 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), 428–439. https://doi.org/10.53363/bureau.v3i1.191

Heppy Endah Palupy. (2011). Privacy and data protection : Indonesia legal framework. Universiteit van Tilburg.

Indonesia Anti Phising Data Exchange (IDADX). (2023). *Laporan aktivitas phishing Q1 2023*.

Kardos, V. (2022). Data protection challenges in the era of artificial intelligence. *Central and Eastern European EDem and EGov Days*, *341*, 285–294. https://doi.org/10.24989/ocg.v341.21

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, *26*(1), 89–120. https://doi.org/10.1007/s11948-018-00081-0

Komarudin, W. D. dan A. (2014). *Perlindungan hak atas privasi di internet-beberapa penjelasan kunci*. Elsam.

Lastdrager, E. E. H. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. In *Crime Science* (Vol. 3, Issue 1). https://doi.org/10.1186/s40163-014-0009-y

Lee, J., Kim, J., Kim, I., & Han, K. (2019). Cyber threat detection based on artificial neural networks using event profiles. *IEEE Access*, *7*, 165607–165626. https://doi.org/10.1109/ACCESS.2019.2953095

Lilis Ekayani. (2023). Perlindungan hukum nasabah terhadap kejahatan pencurian data pribadi (phising) di lingkungan perbankan. *Journal Of Lex Philosophy (JLP)*, *4*(1), 22–40. https://doi.org/10.52103/jlp.v4i1.1485.

M. Al-diabat. (2016). Detection and prediction of phishing websites using classification mining techniques. *International Journal of Computer Applications*, *147*(5). https://doi.org/10.5120/ijca2016911061.

Mahameru, D., Nurhalizah, A., Wildan, A., Badjeber, M., & Rahmadia, M. (2023). Implementasi UU perlindungan data pribadi terhadap keamanan informasi identitas di Indonesia. *Jurnal Esensi Hukum*, *November 2023.*

*https://www.researchgate.net/publication/375989201_*Implementasi_Uu_Perlindungan_Data_Pribadi_Terhadap_Keamanan_Informasi_Identitas_Di_Indonesia.

Makarim, E. (2004a). *Kompilasi hukum telematika, Jakarta hlm. 3. Lihat juga M. Arsyad Sanusi, Teknologi Informasi & Hukum E-commerce, PT. Dian Ariesta, Jakarta, 2004*. PT. Raja Grafindo Perkasa.

Masyhar, A., & Emovwodo, S. O. (2023). Techno-prevention in counterterrorism: between countering crime and human rights protection. *Journal of Human Rights, Culture and Legal System*, *3*(3), 625-655. https://doi.org/10.53955/jhcls.v3i3.176

Meurisch, C., & Mühlhäuser, M. (2022). Data Protection in AI services. *ACM computing surveys*, *54*(2), 1–38. https://doi.org/10.1145/3440754

Mihai, I.-C. (2012). Overview on phishing attacks. *International Journal of Information Security and Cybercrime*, *1*(2), 61-67. https://doi.org/10.19107/ijisc.2012.02.07

Muir, A., & Oppenheim, C. (2002). National information policy developments worldwide IV: Copyright, freedom of information and data protection. *Journal of Information Science*, *28*(6), 467-481. https://doi.org/10.1177/016555150202800603

Pagallo, U. (2011). Designing data protection safeguards ethically. *Information*, *2*(2), 247–265. https://doi.org/10.3390/info2020247

Petar Radanliev, & Omar Santos. (2023). Ethics and responsible AI deployment. *Frontiers in Artificial Intelligence*, *7*(1).

Purwaningsih, R., & Putranto, R. D. (2023). Tinjauan yuridis terhadap penetapan locus delicti dalam kejahatan dunia maya (cyber crime) berkaitan dengan upaya pembaharuan hukum pidana di Indonesia. *Mimbar Keadilan*, *16*(1), 130–138. https://doi.org/10.30996/mk.v16i1.8021

Rangaraju, S. (2023). Secure by intelligence: enhancing products with AI-driven security measures. *EPH - International Journal of Science And Engineering*, *9*(3), 36–41. https://doi.org/10.53555/ephijse.v9i3.212

Rao, R. S., & Pais, A. R. (2019). Detection of phishing websites using an efficient feature-based machine learning framework. *Neural Computing and Applications*, *31*(8), 3851–3873. https://doi.org/10.1007/s00521-017-3305-0

Riskawati, A. A. A. dan. (2016). "Penanganan kasus cybercrime di Kota Makassar (studi pada kantor kepolisian resort Kota Besar Makassar). *Jurnal Supremasi*, *10*. https://doi.org/10.26858/supremasi.v11i1.3023.

Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. *Expert Systems with Applications*, *117*, 345–357. https://doi.org/10.1016/j.eswa.2018.09.029

Sameen, M., Han, K., & Hwang, S. O. (2020). PhishHaven-an efficient real-time AI phishing URls detection system. *IEEE Access*, *8*, 83425-83443. https://doi.org/10.1109/ACCESS.2020.2991403

Selyanin, Y. (2021). Budget funding priorities and development prospects of the US artificial intelligence. *Analysis and Forecasting. IMEMO Journal*, *3*, 65–93. https://doi.org/10.20542/afij-2021-3-65-93

Setiawan, D. A. (2020). Cyber terrorism and its prevention in Indonesia. *Jurnal Media Hukum*, *27*(2). https://doi.org/10.18196/jmh.20200156

Situmeang, S. M. T. (2021). Penyalahgunaan data pribadi sebagai bentuk kejahatan sempurna dalam perspektif hukum siber. *SASI*, *27*(1), 38. https://doi.org/10.47268/sasi.v27i1.394

Sulistianingsih, D., Ihwan, M., Setiawan, A., & Prabowo, M. S. (2023). Tata kelola perlindungan data pribadi di era metaverse (telaah yuridis undang-undang perlindungan data pribadi). *Masalah-Masalah Hukum*, *52*(1), 97–106. https://doi.org/10.14710/mmh.52.1.2023.97-106

Tan, J. G. (2008). A Comparative study of the APEC privacy framework- a new voice in the data protection dialogue? *Asian Journal of Comparative Law*, *3*, 1–44. https://doi.org/10.1017/S2194607800000181

Tarafdar, S. A., & Fay, M. (2018). Freedom of information and data protection acts. *Innovait: Education and Inspiration for General Practice*, *11*(1), 48–54. https://doi.org/10.1177/1755738017735139

Tchinaryan, E. O., Lavrentieva, M. S., Kuchenin, E. S., & Neznamova, A. A. (2019). Digital technologies of the European Union in personal data protection. *International Journal of Innovative Technology and Exploring Engineering*, *8*(12), 3600–3604. https://doi.org/10.35940/ijitee.L3798.1081219

Teguh Prasetyo. (2013). *Hukum pidana*. PT. Raja Grafindo Persada.

Tripathi, K., & Mubarak, U. (2020). Protecting privacy in the era of artificial intelligence. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3560047

Urban, T., Tatang, D., Degeling, M., Holz, T., & Pohlmann, N. (2018). *The unwanted sharing economy: An analysis of cookie syncing and user transparency under GDPR*. https://doi.org/10.1145/3320269.3372194

Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan yuridis terhadap perlindungan data pribadi dari aspek pengamanan data dan keamanan siber. *Jurnal Multidisiplin Indonesia*, *2*(3), 654-666. https://doi.org/10.58344/jmi.v2i3.157

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, *45*(8), 1146–1166. https://doi.org/10.1177/0093650215627483

Wachter, S., & Mittelstadt, B. D. (2018). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, 494–620. https://doi.org/10.31228/osf.io/mu2kf.

Wahyu Sudrajat. (2021). Relativitas peraturan dalam hukum. *Https://Www.Hukumonline.Com/Berita/a/Relativitas-Peraturan-Dalam-Hukum-Lt60e5205a1d473/.*

Weber, R. H. (2010). Internet of things – new security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23-30. https://doi.org/10.1016/j.clsr.2009.11.008

Wu, W., & Liu, S. (2023). Compliance costs of AI technology commercialization: A field deployment perspective. *Computer Science, Business, Economics.* DOI:10.48550/arXiv.2301.13454

Xun Dong, Clark, J. A., & Jacob, J. L. (2008). User behaviour based phishing websites detection. *2008 International Multiconference on Computer Science and Information Technology*, 783-790. https://doi.org/10.1109/IMCSIT.2008.4747332

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences (BECOSS) Journal*, *1*(1), 147–154.https://doi.org/10.21512/becossjournal.v1i1.6030

Yuniarti S., AM Ramli, SD Rosadi, D. B. (2023). The new chapter of Indonesia's data protection on digital economy perspective. *Journal of Southwest Jiaotong University*, *58*(3). https://doi.org/10.35741/issn.0258-2724.58.3.9

Yuspin, W., Wardiono, K., Budiono, A., & Gulyamov, S. (2022). The law alteration on artificial intelligence in reducing Islamic bank's profit and loss sharing risk. *Legality : Jurnal Ilmiah Hukum*, *30*(2), 267-282. https://doi.org/10.22219/ljih.v30i2.23051

Article History
Submitted 5 November 2023 - Revision Required 17 May 2024 - Accepted 21 November 2024