Jurnal Idea Hukum

Vol. 11 Issue 2, October 2025
E-ISSN 2442-7454 P-ISSN 2442-7241
DOI: 10.20884/1.jih.2025.11.2.651

When Artificial Intelligence Becomes a Criminal Tool: Urgency of Criminal Law Policy Against Data Theft in Indonesia

Helmi Gunawan
Universitas Jenderal Soedirman
✉ gunawanhelmoi212@gmail.com

Submitted : 07/07/2025
Revised : 19/09/2025
Accepted : 13/11/2025

Abstract
Personal data has become a valuable asset in the present era. The security of personal data is an absolute necessity that must be considered by everyone to be protected from all existing threats. Artificial Intelligence (AI) is increasingly developing and becoming an integral part of modern society. This article aims to identify the various forms of acts that can be committed in AI-based data theft and to examine the national criminal law policies addressing AI-based data theft offenses. The article adopts a normative juridical approach through legislation and conceptual analysis, with a descriptive-analytical specification. The findings indicate that the most common form of data theft involves the dissemination of deepfake. Indonesian regulations have not comprehensively or specifically addressed AI in their legal frameworks. The Personal Data Protection and the Electronic Information and Transactions Law are the primary regulations applied in data theft cases; however, these laws do not provide detailed explanations related to AI. Perpetrators generally use deepfake technology as a method to commit data theft. The establishment of specific regulations to address AI usage from a criminal law perspective aims to prevent offenses that utilize AI as an aiding tool. The article's results demonstrate that Indonesia's criminal law regulations are currently inadequate to anticipate the misuse of AI in cybercrime, thus necessitating the creation of lex specialis norms that clarify the position of AI within the structure of criminal liability.

Keywords: Personal Data Protection; Artificial Intelligence; Data Theft.

Introduction

Personal data theft constitutes a violation of security and privacy that can cause serious impacts. These impacts include account exploitation, spam, and substantial material losses.[1] The rise in personal data theft correlates with the increasing number of electronic device users and frequent internet usage, to the extent that human life today is inseparable from the internet.[2] SAFEnet (South East Asia Freedom of Expression Network) identifies three motives behind personal data theft: economic, political, and intimidation. In the economic motive, perpetrators illegally trade personal data for profit; in the political motive, acts are committed for power and political purposes; and in the intimidation motive,

[1] Dian Rahmawati, Muhammad Darriel Aqmal Aksana, and Siti Mukaromah, "Privasi Dan Keamanan Data Di Media Sosial: Dampak Negatif Dan Strategi Pencegahan," *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi* 3, no. 1 (November 2023): 571–80, https://doi.org/10.33005/sitasi.v3i1.354.
[2] Fiqqih Anugerah and Tantimin Tantimin, "Pencurian Data Pribadi Di Internet Dalam Perspektif Kriminologi," *Jurnal Komunikasi Hukum (JKH)* 8, no. 1 (February 2022): 419–35, https://doi.org/10.23887/jkh.v8i1.45434.

perpetrators disclose and spread personal data to instill fear in the victims.[3] Therefore, preventive measures are necessary to avoid malicious motives that could lead to harmful actions affecting victims.

Artificial Intelligence (AI), or "Kecerdasan Artifisial", etymologically consists of the phrases "artificial" and "intelligence.". According to the KBBI, "artificial" means unnatural or man-made,[4] while "intelligence" is defined as the perfection of intellectual development.[5] According to Pratama (2023), AI refers to technology aimed at developing computers that possess human-like intelligence.[6] Common AI examples used in daily life include ChatGPT, Perplexity, Gemini, and others.[7] AI is also categorized into two types: Narrow AI, which is a weak system, and General AI, which approaches human performance.[8] From these definitions, it is understood that AI is a system created to facilitate human tasks, enabling them to be completed more quickly and efficiently.

AI is supported by systems capable of gathering data from various sources to "learn" and make decisions or predictions. AI can process personal data such as names, addresses, biometric data, economic transactions, and social media usage habits.[9] Dark Readith (2018) mentioned that "Alexa," a virtual assistant widely used, is known to secretly record conversations and send them to random contacts without consent.[10] The developer of the AI application "FaceApp" also states in its terms of service that the company has the right to manage anything created by users.[11] In practice, AI can recognize patterns that infer personal behavior and preferences, often without the data owner's knowledge.

Previous articles on Artificial Intelligence (AI) have not deeply explored the relationship between AI and personal data theft. First, Kaur (2023) classified common AI types based on the NIST cybersecurity framework using thematic analysis.[12] Second, King (2023) studied "AI-Crime" (AIC), focusing on automated fraud targeting social media users.[13] Third, Carpenter (2025) investigated aggressive crimes and introduced the concept of "cyber-aggression," exploring

[3] CNN Indoneisa, "SAFEnet Ungkap 3 Motif Pencurian Data Pribadi," 2019.
[4] KBBI, "Pengertian Artifisial," 2024.
[5] KBBI, "Pengertian Kecerdasan," 2024.
[6] Arya Satya Pratama et al., "Pengaruh Artificial Intelligence, Big Data Dan Otomatisasi Terhadap Kinerja SDM Di Era Digital," *Jurnal Publikasi Ilmu Manajemen* 2, no. 4 (2023): 108–23, https://doi.org/10.55606/jupiman.v2i4.2739.
[7] Coursera, "What Is Artificial Intelligence? Definition, Uses, and Types," 2024, https://www.coursera.org/articles/what-is-artificial-intelligence.
[8] Coursera.
[9] Andhika, "Bagaimana AI Dapat Membocorkan Data Pribadi Anda?," 2024.
[10] Klaudia Sisilia et al., "Ancaman Risiko Keamanan Theft Identity Pada Aplikasi Berbasis Artificial Intelligence Dalam Perspektif Lifestyle Exposure Theory" 8, no. 2 (n.d.).
[11] Coursera, "What Is Artificial Intelligence? Definition, Uses, and Types."
[12] Ramanpreet Kaur, Dušan Gabrijelčič, and Tomaž Klobučar, "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions," *Information Fusion* 97 (September 2023): 101804, https://doi.org/10.1016/j.inffus.2023.101804.
[13] Thomas C. King et al., "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions," *Science and Engineering Ethics* 26, no. 1 (February 2020): 89–120, https://doi.org/10.1007/s11948-018-00081-0.

challenges related to AI-based aggression within the conventional framework of international criminal liability.[14] The novelty of this article lies in revealing national criminal law policy responses to AI-facilitated personal data theft. Law Number 27 of 2022 on Personal Data Theft states in the preamble that personal data protection is a form of human rights that requires a legal basis to provide security for personal data. This article is based on several assumptions: First, AI-based data theft in the future will increasingly threaten the privacy of individuals and companies. Second, AI has yet to be significantly regulated, making it difficult to prove in law enforcement practice.

Research Problems

1. What are the forms of AI-Based data theft?
2. How does national criminal law policy address AI-Based data theft?

Method

The research method used in this article is the normative juridical method. Essentially, an article adopting the normative juridical method involves examining the internal aspects of positive law.[15] Peter Mahmud Marzuki, in his book, defines normative legal research as "a method of studying legislation based on the hierarchy of laws and regulations (vertical) as well as the harmonious relationship among laws and regulations (horizontal). [16] This article employs several approaches, namely the conceptual approach, statutory approach, and comparative approach. The conceptual approach is used to analyze the theoretical understanding of AI-based data theft crimes, including the principles of classical and modern criminal law in responding to developments in cybercrime. This approach also serves as a basis for interpreting the scope of criminal liability in acts involving algorithms, automated systems, or artificial intelligence.

The statutory approach is used operationally by reviewing the substance of applicable positive law in Indonesia, such as the Criminal Code *(Kitab Undang-Undang Hukum Pidana - KUHP)* to assess the relevance of conventional crime formulations to digital data theft phenomena; the Electronic Information and Transactions Law *(Undang-Undang Informasi dan Transaksi Elektronik - ITE)* to evaluate the scope of regulations concerning illegal access, theft, and misuse of electronic data; and Law No. 27 of 2022 on Personal Data Protection *(Undang-Undang Pelindungan Data Pribadi – PDP)* as a new norm providing legal protection guarantees for data owners. The analysis is conducted by comparing norms, assessing the compatibility among regulations, and identifying potential

[14] Christine Carpenter, "Whose [Crime] Is It Anyway?," *Journal of International Criminal Justice* 23, no. 1 (March 2025): 69–86, https://doi.org/10.1093/jicj/mqae055.
[15] Kornelius Benuf and Muhamad Azhar, "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer," *Gema Keadilan* 7, no. 1 (2020): 20–33.
[16] Peter Mahmud Marzuki, *Pengantar Ilmu Hukum*, ed. Kencana (Jakarta, 2008).

regulatory gaps or overlaps in addressing AI-based data theft. Through this method, the research not only identifies applicable rules but also examines how these legal norms can be implemented, whether they can anticipate the evolving modes of AI-facilitated data theft, and to what extent they effectively provide legal certainty for society.

Discussion

1. Forms of Acts in AI-Based Data Theft

Data theft and Artificial Intelligence (AI) have not yet been legally defined as juridical terms within the regulatory framework in Indonesia. There is currently no legislation that explicitly formulates these terms. In the context of cyberspace and personal data protection, regulations have been established under *the ITE Law* enacted in 2008, 2016, and 2023, and also under *the PDP Law* of 2022. Within these two laws, forms of data theft are classified as follows:

Table 1. Personal Data Theft in Legislation

No	*The ITE Law*	*The PDP Law*
1	Article 30 paragraph (2): Accessing an Electronic System by any means with the intent to obtain Electronic Information.	Article 67 paragraph (1): Collecting personal data that does not belong to oneself with the intent to benefit oneself or others which may cause harm to the personal data subject
2	Article 30 paragraph (3): Accessing an Electronic System by any means in violation of security systems.	Article 67 paragraph (2): Disclosing personal data that does not belong to oneself.
3		Article 67 paragraph (3): Using personal data that does not belong to oneself

Source: the ITE Law and the PDP Law

There are distinct differences between the two laws in formulating acts of personal data theft. First, the act of personal data theft as stated in the ITE Law resembles the formulation of theft offenses in the Criminal Code, specifically ordinary theft as regulated under Article 362 of the KUHP, which is analogous to Article 30 paragraph (2) of the ITE Law, and qualified theft under Article 363 of the KUHP, similar to Article 30 paragraph (2) of the ITE Law. In practice at the courts, this article found that cases involving personal data theft tend to use Article 67 paragraph (1) of the PDP Law, as evidenced in Decisions No. 1208/Pid.Sus/2024/PN Pbr and No. 1134/Pid.Sus/2024/PN Tjk.

The cases of personal data theft from victims within information systems remain consistent regardless of whether AI is used in the execution. Socially, AI usage in Indonesia tends to be employed for personal data theft, as seen from the widespread application of AI in searching for information.[17] According to data released by the National Cyber and Crypto Agency (BSSN), reports related to

[17] Marzuki.

phishing incidents are low, indicating a generally low public awareness regarding stolen personal data.[18] These BSSN data correspond with police data, which indicate that personal data theft is not among the highest reported cases handled by the police.[19] Although reports of personal data theft remain infrequent, other cybercrime complaints or reports are related to the theft or misuse of others' personal data, including acts like doxxing.

Privacy rights are a crucial element of individual freedom and dignity. Potential privacy violations may occur in practices such as mass collection of personal data (digital dossier), direct marketing, social media, implementation of e-KTP programs, e-health projects, and cloud computing activities.[20] The regulations under the ITE Law are considered inadequate to face the increasingly sophisticated and evolving digital era challenges.[21] The ITE Law only provides basic rules regarding consent for personal data use and prohibits the misuse of electronic information. There are no detailed provisions on data management, storage, or deletion.[22] The academic manuscript on the Personal Data Protection Bill explains that the purpose of establishing data protection regulations is to safeguard consumer interests and provide economic benefits for Indonesia.[23] This bill also regulates personal data protection that can minimize threats of misuse in banking industries and electronic marketplaces.

Numerous personal data theft cases have occurred, resulting in losses for the data subjects. Despite the many cases causing harm to personal data subjects, there has been no continuation of legal proceedings in court regarding sanctions against perpetrators of data theft. The following are examples of personal data theft cases that have occurred:

Table 2. Personal Data Breach Cases

Case	Year	Description
BPJS Kesehatan Data Leak[24]	2021	Data of 279 million BPJS Kesehatan participants is suspected to have been leaked and traded on the dark web. The leaked information includes names, phone numbers, addresses, health histories, and personal photographs.
E-Commerce Platform Data Leak[25]	2019-2020	During this period, approximately 105 million user data records from various e-commerce platforms were stolen and traded on the dark web. The stolen data includes User IDs, email addresses, usernames, date of birth, gender, phone numbers, and passwords of victims.

[18] BSSN, "Laporan Bulanan Publik," 2023.
[19] Patroli Siber, "Jumlah Laporan Polisi Yang Dibuat Masyarakat," Bareskrim Polri, 2025.
[20] BPHN, "NA Perlindungan Data Pribadi," n.d.
[21] JDIH Kota Semarang, "Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (PDP): Menjaga Kemanan Dan Privasi Data Warga Negara," 2024.
[22] JDIH Kota Semarang.
[23] BPHN, "NA Perlindungan Data Pribadi."
[24] Achmad Firdaus, "Kasus Kebocoran Data Pribadi Di Indonesia: 10 Kejadian Terbesar Yang Perlu Diketahui," 2024.
[25] Redaksi, "Menolak Lupa! Ini 10 Daftar Kasus Kebocoran Data Pribadi Di Indonesia," 2024.

NPWP Data Leak[26]	2024	This case went viral at the end of 2024, involving the leak and sale of around 6 million NPWP data, including high-ranking officials and public figures.

Sources: Medcom.com; Balinesia.id; News.detik.com.

Artificial Intelligence (AI) can be used to search for detailed information about a particular matter. This allows irresponsible parties to seek personal data of individuals for personal gain. The following are several ways AI is used to steal someone's personal data, including:[27]

a. Spreading Deepfake

Deepfake is a video or audio clip created by AI that appears very realistic. In practice, deepfake can be used by perpetrators who send videos purportedly from a superior at the victim's workplace requesting the victim's personal information. Another common method is that hackers or perpetrators use deepfake to spread negative news about a company, causing security disruptions so that the company's personal data can be stolen by the perpetrators;

b. Solving Captcha

AI algorithms can quickly analyze and respond to images similar to human abilities. This is exploited by perpetrators to hack through security captchas using AI;

c. Keylogging

Some AI tools can "listen" to keystrokes and identify user passwords with up to 95% accuracy. Although it requires extensive training for AI, once the machine learning process is complete, perpetrators can use AI to crack victims' passwords.

The most commonly used method by personal data thieves is spreading deepfake. In a December 2024 case involving two perpetrators who were arrested for opening accounts at private banks using other people's personal data without permission, the theft was assisted by AI.[28] In a press conference, the Metro Jaya Police stated, "After an in-depth investigation of several accounts, it was detected that during the account opening verification process through the application, the perpetrators used AI assistance." AI was used to fabricate face verification videos, so the system identified them as the legitimate owners of the data used.

[26] Matius Alfons Hutajulu, "Dugaan Kebocoran Data NPWP, Anggota DPR: Ini Ancaman Serius," 2024.
[27] Kelle White, "7 Ways AI Can Be Used by Hackers to Steal Personal Information," 2024.
[28] Baharudin Al Farisi & Abdul Haris Maulana, "2 Pria Buka Rekening Bank Dengan Data Pribadi Orang Lain, Rekayasa Pakai AI," 2025.

In the case described above, the suspects were charged under several criminal provisions as follows:[29]

a. Article 51 Paragraph (1) in conjuction with Article 35 of the ITE Law

Unauthorized or unlawful acts of manipulation, creation, alteration, deletion, or destruction of Electronic Information and/or Electronic Documents with the intention that the Electronic Information and/or Electronic Documents are perceived as authentic data;

b. Article 48 Paragraph (1) in conjuction with Article 32 Paragraph (1) of the ITE Law

Unauthorized or unlawful acts in any manner to change, add, reduce, transmit, damage, delete, move, or hide someone else's or public Electronic Information and/or Electronic Documents, based on Article 48 paragraph (1) in conjunction with Article 32 paragraph (1) of the ITE Law;

c. Article 67 in conjuction with Article 65 Paragraph (1) of the Personal Data Protection Law (PDP Law)

Everyone is prohibited from unlawfully obtaining or collecting Personal Data that is not their own with the intention of benefiting themselves or others, which may cause harm to the Personal Data Subject;

d. Article 67 Paragraph (2) in conjuction with Article 65 Paragraph (2) of the Personal Data Protection Law (PDP Law)

Every person is prohibited from unlawfully disclosing Personal Data that does not belong to them.

The core of the case, according to the Investigator, involves fabricating a facial verification video to open a bank account. Based on the construction of the articles in the official release, the legal points are as follows:

a. The use of AI to fabricate facial verification videos for the purpose of opening accounts constitutes manipulation of electronic documents and/or electronic information as stipulated in Article 51 paragraph (1) in conjunction with Article 35 of the ITE Law;

b. The use of AI to fabricate facial verification videos for account opening constitutes altering electronic information and/or electronic documents belonging to others, based on Article 48 paragraph (1) in conjunction with Article 32 paragraph (1) of the ITE Law;

c. The use of AI to fabricate facial verification videos for account opening constitutes acts of unlawfully obtaining or collecting Personal Data not belonging to oneself with the intent to benefit oneself or others, which

[29] Maulana.

may cause harm to the Personal Data Subject, as regulated in Article 67 in conjunction with Article 65 paragraph (1) of the PDP Law;

d. The use of AI to fabricate facial verification videos for account opening constitutes disclosure of Personal Data not belonging to the actor, based on Article 67 paragraph (2) in conjunction with Article 65 paragraph (2) of the PDP Law.

Currently, no article officially defines Artificial Intelligence (AI). The closest provision is Article 10 paragraph (1) of the PDP Law, which states, "The Personal Data Subject has the right to object to decisions based solely on automated processing, including profiling, which produce legal effects or significantly affect the Personal Data Subject." The explanation of this article defines profiling as "activities of identifying a person, including but not limited to employment history, economic condition, health, personal preferences, interests, reliability, behavior, location, or movements of the personal data subject electronically." Article 10 is thus the closest provision to the definition of AI-based Personal Data Theft under the principle of extensive interpretation, which broadens the meaning of terms within the Law to include relevant phenomena. The phrase "...decisions based solely on automated processing..." within Article 10, when linked to the broad interpretation of "automated processing," can be associated with AI use. Processing that requires consent from the personal data subject indicates that Article 10 of the PDP Law adopts the principle of accountability.

Personal data is indeed closely associated with *the ITE Law* and *the PDP Law*. Both regulations do not specifically regulate the use of Artificial Intelligence, although ideally AI should be regulated within Indonesia's positive legal system, which can be implemented in specific AI legislation as a legal subject such as a legal entity.[30] In practice, Indonesia has only formulated circulars regarding the use of AI, such as:

a. Indonesian National Artificial Intelligence Strategy (Stranas KA)[31]

Formulated by the Agency for the Assessment and Application of Technology (BPPT) in 2020, it establishes Ethical Principles and Policies for Artificial Intelligence in Indonesia based on the following principles:

1) Human oversight;
2) Technical robustness and safety;
3) Data governance and privacy;
4) Transparency;
5) Social and environmental well-being; and
6) Diversity, non-discrimination, and fairness.

[30] Bagus Gede Ari Rama, Dewa Krisna Prasada, and Kadek Julia Mahadewi, "Urgensi Pengaturan Artificial Intelligence (AI) Dalam Bidang Hukum Hak Cipta Di Indonesia," *JURNAL RECHTENS*, 2023, https://doi.org/10.56013/rechtens.v12i2.2395.
[31] BPPT, "Strategi Nasional Kecerdasan Artifisial Indonesia 2020-2045," 2020.

b. Guidelines for a Responsible and Trustworthy Artificial Intelligence Code of Ethics in the Financial Technology Industry[32]

Formulated by the Financial Services Authority (OJK) in 2023, this guideline aims to mitigate risks and optimize AI in the fintech industry. It provides a code of conduct serving as guidance for fintech providers and related parties to ensure that AI usage complies with the following principles:

1) Based on Pancasila;
2) Beneficial;
3) Fair and accountable;
4) Transparent and explicable;
5) *R*obustness and security.

AI is a complex system that does not merely provide quick and practical answers to users. Generally, the working mechanism of AI is as follows:[33]

a. Data Collection

Data is the primary raw material to train AI models. The collected data can come from various sources such as databases or internet users who publish writings or works;

b. Data Cleaning and Preprocessing

This process is necessary because raw data often contains errors or missing values from the original provision. Data cleaning aims to correct these errors and ensure that the data used for training AI models is of high quality. Preprocessing transforms the data into a format acceptable by AI algorithms;

c. Algorithm Selection

Various types of algorithms can be used in AI, each with advantages and disadvantages. For example, AI used for classification tasks may employ machine learning, decision trees, or random forests. Choosing the right algorithm is essential since the system must understand the users' intentions;

d. Model Training

In this process, preprocessed data is used to train the AI model. Training involves adjusting model parameters to perform specific tasks with high accuracy. This usually requires extensive iteration and optimization techniques to achieve the best results;

[32] Otoritas Jasa Keuangan, "Panduan Kode Etik Kecerdasan Buatan (Artificial Intelligence) Yang Bertanggung Jawab Dan Terpercaya Di Industri Teknologi Finansial," 2023.
[33] Verihubs, "Mengenal Cara Kerja AI: Dasar-Dasar Kecerdasan Buatan," 2024.

e. Model Evaluation

Evaluation measures the model's accuracy, precision, recall, and F1 score. Separate test data is also used to avoid overfitting during training;

f. Model Refinement

Refinement involves various techniques such as parameter tuning, adding more training data, or using different algorithms to improve the model;

g. Model Deployment

Deployment involves implementing the AI model in a production environment for specific tasks. This includes integrating the model with existing systems and ensuring efficient operation;

h. Model Monitoring and Maintenance

The final process is monitoring and maintaining the model to ensure it continues functioning well and does not degrade over time. This may involve periodic updates with new data to keep the model relevant and accurate.

Large Language Models (LLM) are a familiar term in the application of AI. Large Language Models are a category of deep learning models trained on large-scale data, enabling them to understand and generate natural language and other types of content to perform various assigned tasks.[34] Large Language Models represent a paradigm shift in artificial intelligence, far surpassing Natural Language Processing (NLP*).*[35] We observe increasingly advanced and evolving AI applications in society, which create numerous opportunities for irresponsible parties to gain personal benefits. Prompt Injection is a form of cyber attack that causes violent or discriminatory responses through command inputs containing illegal instructions to the Large Language Model.[36] Prompt Injection involves the manipulation of Large Language Models by bypassing filters or using complex commands, resulting in the Large Language Models carrying out undesirable and unlawful actions.[37] In this context, AI user data is vulnerable to theft by irresponsible actors.

The theft of personal data constitutes an act that causes destructive impacts on both the state and society, thus necessitating stringent criminal sanctions against offenders. Legal efforts to address criminal acts are essentially divided into penal measures, which emphasize repressive efforts, and non-penal measures, which emphasize preventive efforts. In practice, the imposition of criminal

[34] Cole Stryker, "What Are LLMs?," 2024.
[35] Seyed Mahmoud Sajjadi Mohammadabadi et al., "A Survey of Large Language Models: Evolution, Architectures, Adaptation, Benchmarking, Applications, Challenges, and Societal Implications," *Electronics* 14, no. 18 (September 2025): 3580, https://doi.org/10.3390/electronics14183580.
[36] Hyeokjin Kwon and Wooguil Pak, "Text-Based Prompt Injection Attack Using Mathematical Functions in Modern Large Language Models," *Electronics* 13, no. 24 (December 2024): 5008, https://doi.org/10.3390/electronics13245008.
[37] Kwon and Pak.

sanctions serves a deterrent effect on offenders, and the formulation of sanctions must be commensurate with the offense committed. The crime of personal data theft can only be effectively addressed through criminal law and not by other forms of law.

During the regulatory formulation stage, a process of criminalization occurs. Criminalization is the process of designating an act as a crime, enabling prosecution and determination of sanctions. The state is obliged to protect and respect the rights of its citizens individually. According to H.L.A. Hart, there are occasions when the state must take the initiative to prohibit an act, hoping that society will develop an attitude of rejection toward that act.[38] The enactment of *the PDP Law* serves as concrete evidence of government participation in the formulation and implementation of the *the PDP Law* as a legal framework regulating the collection, processing, and storage of personal data. In this regard, the state is present in its efforts to safeguard the personal data of the public.

2. National Criminal Law Policy in Addressig AI-Based Data Theft

Data theft within the framework of the national criminal law policy, as stipulated in the Penal Provisions chapter of *the PDP Law* , is not classified as a juridical term or legal offense title. The same applies to Artificial Intelligence (AI), for which there is currently no legislation defining AI. Definitions of AI have been formulated outside Indonesia, notably by the European Union through the Artificial Intelligence Act (AI Act) 2024, which provides the following formulation:[39]

> *An AI system is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.*

The act of stealing data using AI can still be prosecuted under several penal provisions found in the Penal Provisions chapter regulated *the ITE Law*, as amended first by Law Number 19 of 2016 and second by Law Number 1 of 2024, and by *the PDP Law*. These two laws define several criminal offenses as follows:

a. Article 46 Paragraph (2) in Conjunction with Article 30 Paragraph (2) of the ITE Law

Any person who fulfills the element of "intentionally and without authorization or unlawfully accessing a computer and/or electronic system by any means with the purpose of obtaining electronic information and/or electronic documents" shall be punished with imprisonment for a maximum

[38] Arief Budiono et al., "Jhon Austin's Positivism Legal Policy: Convergence of Natural Law," *International Journal of Multicultural and Multireligious Understanding* 8, no. 9 (September 2021): 401, https://doi.org/10.18415/ijmmu.v8i9.3058.
[39] Official Journal Of European Union, "Artificial Intelligence Act," 2024.

of 7 (seven) years and/or a fine of up to IDR 700,000,000.00 (seven hundred million rupiah).

b. Article 46 Paragraph (3) in Conjunction with Article 30 Paragraph (3) of ITE Law

Any person who fulfills the element of "intentionally and without authorization or unlawfully accessing an electronic system by any means in violation of security systems" shall be punished with imprisonment for a maximum of 8 (eight) years and/or a fine of up to IDR 800,000,000.00 (eight hundred million rupiah).

c. Article 67 Paragraph (1) of PDP Law

Any person who intentionally and unlawfully obtains or collects personal data that is not theirs with the intent to benefit themselves or others, thereby causing harm to the data subject as referred to in Article 65 paragraph (1), shall be punished with imprisonment for a maximum of 5 (five) years and/or a fine of up to IDR 5,000,000,000.00 (five billion rupiah).

d. Article 67 Paragraph (2) of PDP Law

Any person who intentionally and unlawfully discloses personal data that is not theirs as referred to in Article 65 paragraph (2) shall be punished with imprisonment for a maximum of 4 (four) years and/or a fine of up to IDR 4,000,000,000.00 (four billion rupiah).

e. Article 67 Paragraph (3) of PDP Law

Any person who intentionally and unlawfully uses personal data that is not theirs as referred to in Article 65 paragraph (3) shall be punished with imprisonment for a maximum of 5 (five) years and/or a fine of up to IDR 5,000,000,000.00 (five billion rupiah).

In Indonesian court practice, personal data theft cases are thus far prosecuted under Article 67 paragraph (1) of *the PDP Law*, as exemplified by Decision No. 1208/Pid.Sus/2024/PN Pbr and Decision No. 1134/Pid.Sus/2024/PN Tjk. In the latest case presented in this article, which involves AI-based data theft through deepfake technology to open bank accounts, the investigators used several criminal charges, one of which was Article 67 paragraph (1) of *the PDP Law*. Therefore, this article identifies Article 67 paragraph (1) of *the PDP Law* as the primary regulation for criminal offenses relating to AI-based personal data theft because it is most frequently applied to prosecute such offenses.

Considering that Article 67 is most often applied to prosecute or charge data theft crimes, the following outlines its advantages and disadvantages. *The PDP Law* contains significant advantages, particularly in its efforts to protect Human Rights. It also adopts principles consistent with the General Data Protection Regulation (GDPR), such as the data controller, data processor, and data subject rights

principles.[40] The *the PDP Law* also imposes strict sanctions, both administrative and criminal, for violations of personal data protection, which range from written warnings, compensation, fines, up to imprisonment for individuals or organizations that violate the provisions.[41] The shortcomings of Article 67 *the PDP Law* include the absence of implementing regulations for *the PDP Law*, resulting in legal uncertainty and regulatory gaps in personal data protection.[42] This uncertainty leads to the potential for multiple interpretations of *the PDP Law* and opens loopholes for increasing crimes against personal data, including AI-based data theft.[43] The court decisions mentioned above regarding data theft cases demonstrate a gap between the normative provisions in the applicable laws and practical realities. Judges must conduct extensive interpretation because the current laws do not explicitly regulate AI-based data theft modalities. This condition highlights the importance of sub-policy applications within policy formulation, specifically the necessity for the initial formulation of penal norms to consider their effective application in courts. Although Article 67 *the PDP Law* has shortcomings, the author argues that Article 67 is appropriate to apply to data theft cases even though it has not fully accommodated AI-based data theft.

In practice, AI can be misused as a tool to assist in the theft of personal data. AI becomes an object of exploitation as a hacking tool to steal and misuse stolen personal data.[44] AI is used as an aid for stealing personal data because it can enhance the effectiveness of data theft.[45] Indonesian regulations have yet to accommodate clear provisions specifically addressing AI-based data theft; law enforcement officials only interpret AI-based personal data theft as conventional theft in general.[46] AI serves as a fairly effective tool in data theft, yet AI-based data theft is still regarded as conventional theft in general.

With the rapid technological advancements, private data has become highly valuable to many people. This forms the basis for the need for regulations on personal data as a balance between the necessity of protecting personal data and the requirements of the government and business actors to obtain and process data for legitimate and reasonable purposes.[47] Article 29 paragraph (1) of the Human

[40] Nur Alfiana Alfitri, Rahmawati Rahmawati, and Firmansyah Firmansyah, "Perlindungan Terhadap Data Pribadi Di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *Journal Social Society* 4, no. 2 (2024): 92–111, https://doi.org/10.54065/jss.4.2.2024.511.
[41] Alfitri, Rahmawati, and Firmansyah.
[42] Alfitri, Rahmawati, and Firmansyah.
[43] Raudhatul Rafasya, Helfira Citra, and Engrina Fauzi, "Perlindungan Hukum Terhadap Konsumen Atas Pencurian Data Pribadi Dalam Transaksi Elektronik," *Jurnal Ilmu Sosial, Humaniora Dan Seni* 2, no. 2 (2023): 29–33, https://doi.org/10.62379/jishs.v2i2.1251.
[44] Muhammad Rizki Kurniarullah et al., "Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: Deepfake Pornografi Dan Pencurian Data Pribadi," *Jurnal Ilmiah Wahana Pendidikan* 10, no. 10 (2024): 534–47, https://doi.org/https://doi.org/10.5281/zenodo.11448813.
[45] Anastasya Zalsabilla Hermawan et al., "Studi Literatur: Ancaman Sernagan Siber Artificial Intelligence (AI) Terhadap Keamanan Data Di Indonesia," *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi* 3, no. 1 (November 2023): 581–91, https://doi.org/10.33005/sitasi.v3i1.363.
[46] Muhammad Labib & Abdul Wahid, *Kejahatan Mayantara (Cyber Crime)* (Bandung: PT. Refika Aditama, 2005).
[47] Badan Pembinaan Hukum Nasional, "Naskah Akademik RUU Perlindugan Data Pribadi," BPHN, 2016.

Rigaht Law 1999 states that every person has the right to personal protection for oneself, family, honor, dignity, and property. This provision is relevant to privacy rights that require recognition as part of human rights that must be protected due to their importance for the development of modern society.[48] The prohibition on collecting or obtaining another person's personal data aims to achieve security, control, and fulfillment of societal welfare.[49] Given that personal data constitutes privacy and is part of human rights, regulations are necessary to prohibit the unauthorized acquisition of another person's personal data.

Perpetrators who take others' personal data may misuse it by deriving benefits from the stolen data. Stolen and aggregated personal data can be used to commit property crimes, such as hacking into financial accounts or accessing valuable assets through the stolen personal data.[50] The dissemination of personal data may result in harm to society as it can be used to access all kinds of information, including financial and other activities.[51] Normatively, *the PDP Law* contains several prohibitions related to benefits obtained for oneself or others, namely:[52]

a. *The PDP Law* explicitly prohibits the acquisition or collection of personal data that does not belong to the rightful owner, with the intent to obtain benefits for oneself or others that may harm the data subject;

b. *The PDP Law* prohibits the creation or use of falsified personal data with the purpose of obtaining benefits for oneself or others, which may potentially harm others.

In the Academic Draft of the Personal Data Protection Bill, the General Explanation states that the protection of personal data is part of human rights protection, and the establishment of regulations concerning the right to privacy over personal data manifests recognition and safeguarding of fundamental human rights.[53] Therefore, collection or acquisition of personal data to benefit oneself or others is prohibited because it implicates harm to the legal subject whose personal data is stolen, simultaneously violating human rights.

Victims whose personal data is stolen cannot derive benefits from that data and face additional obligations undesired by them. The Academic Draft of the Personal Data Protection Bill explains that privacy violations result in harms that

[48] Badan Pembinaan Hukum Nasional.
[49] Delasnova S. S. Lumintang Taufik Hidayat Telaumbanua, Deasy Soekromo, "Perlindungan Hukum Bagi Pengguna Media Sosial Terhadap Penyalahgunaan Data Pribadi Terkait Hak Privasi Menurut Hukum Positif," *Jurnal Fakultas Hukum Unsrat* 13, no. 01 (2024).
[50] Diyu Sulaeman & Anyelir Puspa Kemala, "Analisis Hukum Terhadap Tindak Pidana Pencurian Identitas Di Indonesia," *Aladalah: Jurnal Politik, Sosial, Hukum Dan Humaniora* 3, no. 2 (2025), https://doi.org/https://doi.org/10.59246/aladalah.v3i2.1258.
[51] Regita Citrazalzabila & Hudi Yusuf, "Pencurian Data Pribadi Di Internet Dari Sudut Pandang Kriminologi," *JICN: Jurnal Intelek Dan Cendikiawan Nusantara* 1, no. 2 (2024).
[52] Ria Juliana Siregar Cindy Gladys Pratiwi Sianturi, Roida Nababan, "Peran Hukum Dalam Melindungi Data Pribadi," *INNOVATIVE: Journal Of Social Science Research* 4, no. 5 (2024): 2607–24.
[53] Badan Pembinaan Hukum Nasional, "Naskah Akademik RUU Perlindugan Data Pribadi."

are greater than physical losses because they interfere with personal life.[54] Such acts can give rise to financial fraud by exploiting the victim's personal data to unlawfully obtain money through financial scams.[55] Besides financial losses, victims of personal data theft often suffer psychological distress and other negative emotional impacts, including anxiety and doubts about the security of their personal information.[56] There are also administrative burdens such as filing police reports, submitting objections to financial institutions, and undertaking digital identity restoration measures.[57] Losses from personal data theft encompass both material and immaterial or psychological damages.

The enactment of the *the PDP Law* in 2022 has made personal data protection more concrete and specific. The *the PDP Law* aims to uphold citizens' rights to security and raise public awareness of the importance of protecting identity information.[58] Its enactment in Indonesia has provided a sufficiently strong legal framework to protect personal data while demonstrating the government's seriousness in regulating this sector.[59] Because of the *the PDP Law*, business actors tend to be more compliant with the obligations regulated therein by implementing better security systems as efforts to protect consumers' personal data.[60] Criticism of *the ITE Law* regarding its inability to fully protect personal data in society and guarantee data security explains the need for more concrete regulations for cases involving personal data theft.[61] Previously, provisions regulating personal data protection were scattered across various laws, leading to inconsistent definitions and scopes of personal data.[62] With the introduction of *the PDP Law*, cases related to personal data theft can be handled using more specific regulations.

The use of *the ITE Law* as the legal basis for imposing sanctions on personal data theft has gradually declined. *the ITE Law* is the main legal foundation regulating electronic transactions in Indonesia,[63] and is not intended specifically to protect personal data, resulting in less effective enforcement against personal

[54] Badan Pembinaan Hukum Nasional.
[55] Saptaning Ruju Paminto, "Perlindungan Hukum Bagi Korban Pencurian Data Dan Informasi Pribadi Di Era Kejahatan Siber," *Jurnal Ilmu Hukum* 2, no. 2 (2025): 25–35, https://doi.org/https://doi.org/10.62017/syariah.
[56] Paminto.
[57] Halimatun Sakdiah et al., "Korelasi Hak & Kewajiban Warga Negara & Negara Dalam Perlindungan Data Pribadi (Menyoroti Kasus Peretasan Data Nasional)" 3, no. 2 (2024): 1303–8, https://doi.org/http://dx.doi.org/10.57235/qistina.v3i2.4049.
[58] Danil Erlangga Mahameru et al., "Implementasi Uu Perlindungan Data" 5, no. 20 (2023): 115–31.
[59] Dewi Asri Puannandini Romadian Amalia, Zaidatul Zulfa, "Efektivitas Penerapan UU Perlindungan Data Pribadi Dalam Transaksi E-Commerce: Tinjauan Terhadap Keamanan Konsumen," *Jurnal Ilmu Hukum* 2, no. 2 (2025): 205–10, https://doi.org/https://doi.org/10.62017/syariah.
[60] Romadian Amalia, Zaidatul Zulfa.
[61] Sepiyah, "Implikasi Hukum Terhadap Perlindungan Data Pribadi Di Era Digital," *Al-Balad: Jurnal Hukum Tata Negara Dan Politik Islam* 2, no. 1 (2022): 26–36.
[62] M Rafifnafia Hertianto, "Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia," *Kertha Patrika* 43, no. 1 (April 2021): 93, https://doi.org/10.24843/KP.2021.v43.i01.p07.
[63] Satrio Ulil Albab, "Perlindungan Hukum Terhadap Data Pribadi Nasabah Penyedia Jasa Pinjaman Bukan Bank Secara Online," *Ethics and Law Journal: Business and Notary* 2, no. 1 (January 2024): 176–82, https://doi.org/10.61292/eljbn.112.

data theft.[64] *The ITE Law* primarily promotes the development of the e-commerce ecosystem, whereas legal instruments such as *the PDP Law* are considered more responsive to societal needs in the digital era.[65] *The ITE Law* offers legal certainty as a lex specialis rule, making the regulation of personal data protection more comprehensive and beneficial from the perspective of normative justice, formulated through harmonization of national, international laws, and the values of Pancasila.[66] *The PDP Law* can replace *the ITE Law* in handling personal data theft crimes as a more concrete and specific regulation.

In the data theft cases mentioned above, Article 67 of the *the PDP Law* is the most frequently applied provision by judges to decide on data theft cases. However, in a 2024 case in Jakarta involving data theft using AI with a deepfake modus operandi, the application of Article 67 *the PDP Law* was considered insufficient to accommodate sanctions against the perpetrators. Therefore, improvements are necessary to recognize AI as a possible subject of the offense within the *the PDP Law*. An example of a sentence structure that could enhance the Article is as follows: "Any person who intentionally and unlawfully obtains or collects personal data that is not theirs with the assistance of others, whether individuals or technologies (Artificial Intelligence), with the intent to benefit themselves or others causing harm to individuals or legal entities, shall be punishable by imprisonment for a maximum of 5 (five) years and/or a fine of up to IDR 5,000,000,000.00 (five billion rupiah)."

Criminal etiology is used to explain the causes of criminal actions, employing Robert K. Merton's Strain Theory. Strain Theory explains that deviant behavior may be influenced by social structures. According to Strain Theory, one cause of crime arises from the failure to achieve goals, which drives criminal acts justified by any means to attain those goals. This theory is often linked to cases involving cultural and social structure imbalances that result in varying levels of deviance within society. In the cases examined in this article, perpetrators tend to commit personal data theft motivated by economic factors, which aligns with Robert K. Merton's adaptation type called Innovation. The cases reviewed in this article are thus relevant to Strain Theory.

The second theory applied is Travis Hirschi's Social Control Theory. Social Control Theory demonstrates that strong social bonds reduce the likelihood of an individual committing crimes. This theory focuses on the restraints and supports that prevent criminal occurrences. Within Social Control Theory, considering that the motive for personal data theft in these cases is economic, the perpetrators'

[64] Hertianto, "Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia."
[65] Hanifan Niffari, "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)," *Jurnal Hukum Dan Bisnis (Selisik)*, 2020, https://doi.org/10.35814/selisik.v6i1.1699.
[66] R. P. P. & Prasetyo Karo Karo, *Pengaturan Perlindungan Data Pribadi Di Indonesia Perspektif Teori Keadilan Bermartabat* (Bandung: Nusa Media, 2020).

behavior is relevant to Hirschi's social bond component called Commitment. Commitment is influenced by the individual behaviors of each person. The cases discussed in this article are consistent with this theory because the predominant motive behind the data thefts is economic or financial gain.

Conclusion

Based on the article and discussion results, several conclusions can be drawn:

1. Data theft cases have occurred frequently and caused losses to the data subjects whose personal data were stolen. Despite the numerous cases and resulting damages to the victims, there has been no further legal process in the courts regarding sanctions against the perpetrators. In practice, the use of AI in Indonesia tends to be employed for stealing personal data, as evidenced by the widespread use of AI to gather information. Forms of AI-based data theft may include spreading deepfake content, breaking captchas, keylogging, and others. The most common method used by AI-based data theft perpetrators is the dissemination of deepfake;
2. Data theft in the national criminal law policy, as set forth in the Penal Provisions chapter of *the PDP Law*, is not classified as a juridical term or offense title. Similarly, Artificial Intelligence (AI) lacks legislative definitions in Indonesian regulations. The act of stealing data using AI can still be prosecuted under several provisions in the Penal Provisions chapter of *the ITE Law* , as amended by Law Number 19 of 2016 and Law Number 1 of 2024, as well as *the PDP Law*. In Indonesian court practice, thus far, personal data theft offenses have been tried under Article 67 paragraph (1) of *the PDP Law* as exemplified by Decision No. 1208/Pid.Sus/2024/PN Pbr and Decision No. 1134/Pid.Sus/2024/PN Tjk. There are no concrete regulations expressly governing AI-based data theft. This absence may lead to the potential for courts to interpret the use of AI as part of manipulative acts within Article 67 *the PDP Law*, although explicit norms have not yet been established.

Suggestion

Based on the article and discussion presented in the previous chapter, the author offers the following recommendations:

1. AI was originally created to support human performance, but it now also poses the potential to be used as a tool for crime, particularly in personal data theft. According to the principle of Lex Certa, lawmakers should formulate legal provisions rigidly to prevent multiple interpretations that could hinder law enforcement officers in applying these laws. Adequate training combined with proper regulation development can help prevent the increasing incidence of AI-assisted data theft..

2. Therefore, it is necessary to revise the existing provisions regarding AI-based data theft in *the ITE Law, the PDP Law Law*, or to enact new, clearer articles or regulations. Moreover, it is important to enhance the understanding of law enforcement personnel about AI usage and the emerging threats due to AI's growing prevalence in society. Thus, synchronization between the formulation and application of criminal policies is key to protecting the public from personal data theft threats.

References

Alfitri, Nur Alfiana, Rahmawati Rahmawati, and Firmansyah Firmansyah. "Perlindungan Terhadap Data Pribadi Di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Journal Social Society* 4, no. 2 (2024): 92–111. https://doi.org/10.54065/jss.4.2.2024.511.

Anastasya Zalsabilla Hermawan, M. Novianto Anggoro, Ditha Lozera, and Asif Faroqi. "Studi Literatur: Ancaman Sernagan Siber Artificial Intelligence (AI) Terhadap Keamanan Data Di Indonesia." *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi* 3, no. 1 (November 2023): 581–91. https://doi.org/10.33005/sitasi.v3i1.363.

Andhika. "Bagaimana AI Dapat Membocorkan Data Pribadi Anda?," 2024.

Anugerah, Fiqqih, and Tantimin Tantimin. "Pencurian Data Pribadi Di Internet Dalam Perspektif Kriminologi." *Jurnal Komunikasi Hukum (JKH)* 8, no. 1 (February 2022): 419–35. https://doi.org/10.23887/jkh.v8i1.45434.

Arya Satya Pratama, Suci Maela Sari, Maila Faiza Hj, Moh Badwi, and Mochammad Isa Anshori. "Pengaruh Artificial Intelligence, Big Data Dan Otomatisasi Terhadap Kinerja SDM Di Era Digital." *Jurnal Publikasi Ilmu Manajemen* 2, no. 4 (2023): 108–23. https://doi.org/10.55606/jupiman.v2i4.2739.

Badan Pembinaan Hukum Nasional. "Naskah Akademik RUU Perlindugan Data Pribadi." BPHN, 2016.

Benuf, Kornelius, and Muhamad Azhar. "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer." *Gema Keadilan* 7, no. 1 (2020): 20–33.

BPHN. "NA Perlindungan Data Pribadi," n.d.

BPPT. "Strategi Nasional Kecerdasan Artifisial Indonesia 2020-2045," 2020.

BSSN. "Laporan Bulanan Publik," 2023.

Budiono, Arief, Dewi Iriani, Nunik Hariyani, and Erma Ullul Janah. "Jhon Austin's Positivism Legal Policy: Convergence of Natural Law." *International Journal of Multicultural and Multireligious Understanding* 8, no. 9 (September 2021): 401. https://doi.org/10.18415/ijmmu.v8i9.3058.

Carpenter, Christine. "Whose [Crime] Is It Anyway?" *Journal of International Criminal Justice* 23, no. 1 (March 2025): 69–86. https://doi.org/10.1093/jicj/mqae055.

Cindy Gladys Pratiwi Sianturi, Roida Nababan, Ria Juliana Siregar. "Peran Hukum Dalam Melindungi Data Pribadi." *INNOVATIVE: Journal Of Social Science Research* 4, no. 5 (2024): 2607–24.

CNN Indoneisa. "SAFEnet Ungkap 3 Motif Pencurian Data Pribadi," 2019.

Coursera. "What Is Artificial Intelligence? Definition, Uses, and Types," 2024. https://www.coursera.org/articles/what-is-artificial-intelligence.

Dian Rahmawati, Muhammad Darriel Aqmal Aksana, and Siti Mukaromah.

"Privasi Dan Keamanan Data Di Media Sosial: Dampak Negatif Dan Strategi Pencegahan." *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi* 3, no. 1 (November 2023): 571–80. https://doi.org/10.33005/sitasi.v3i1.354.

Diyu Sulaeman & Anyelir Puspa Kemala. "Analisis Hukum Terhadap Tindak Pidana Pencurian Identitas Di Indonesia." *Aladalah: Jurnal Politik, Sosial, Hukum Dan Humaniora* 3, no. 2 (2025). https://doi.org/https://doi.org/10.59246/aladalah.v3i2.1258.

Firdaus, Achmad. "Kasus Kebocoran Data Pribadi Di Indonesia: 10 Kejadian Terbesar Yang Perlu Diketahui," 2024.

Gede Ari Rama, Bagus, Dewa Krisna Prasada, and Kadek Julia Mahadewi. "Urgensi Pengaturan Artificial Intelligence (AI) Dalam Bidang Hukum Hak Cipta Di Indonesia." *JURNAL RECHTENS*, 2023. https://doi.org/10.56013/rechtens.v12i2.2395.

Hertianto, M Rafifnafia. "Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia." *Kertha Patrika* 43, no. 1 (April 2021): 93. https://doi.org/10.24843/KP.2021.v43.i01.p07.

Hutajulu, Matius Alfons. "Dugaan Kebocoran Data NPWP, Anggota DPR: Ini Ancaman Serius," 2024.

JDIH Kota Semarang. "Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (PDP): Menjaga Kemanan Dan Privasi Data Warga Negara," 2024.

Karo Karo, R. P. P. & Prasetyo. *Pengaturan Perlindungan Data Pribadi Di Indonesia Perspektif Teori Keadilan Bermartabat*. Bandung: Nusa Media, 2020.

Kaur, Ramanpreet, Dušan Gabrijelčič, and Tomaž Klobučar. "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions." *Information Fusion* 97 (September 2023): 101804. https://doi.org/10.1016/j.inffus.2023.101804.

KBBI. "Pengertian Artifisial," 2024.

———. "Pengertian Kecerdasan," 2024.

King, Thomas C., Nikita Aggarwal, Mariarosaria Taddeo, and Luciano Floridi. "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions." *Science and Engineering Ethics* 26, no. 1 (February 2020): 89–120. https://doi.org/10.1007/s11948-018-00081-0.

Kwon, Hyeokjin, and Wooguil Pak. "Text-Based Prompt Injection Attack Using Mathematical Functions in Modern Large Language Models." *Electronics* 13, no. 24 (December 2024): 5008. https://doi.org/10.3390/electronics13245008.

Mahameru, Danil Erlangga, Aisyah Nurhalizah, Ahmad Wildan, Mochamad Haikal, and Mohamad Haikal Rahmadia. "Implementasi Uu Perlindungan Data" 5, no. 20 (2023): 115–31.

Marzuki, Peter Mahmud. *Pengantar Ilmu Hukum*. Edited by Kencana. Jakarta, 2008.

Maulana, Baharudin Al Farisi & Abdul Haris. "2 Pria Buka Rekening Bank Dengan Data Pribadi Orang Lain, Rekayasa Pakai AI," 2025.

Muhammad Labib & Abdul Wahid. *Kejahatan Mayantara (Cyber Crime)*. Bandung: PT. Refika Aditama, 2005.

Niffari, Hanifan. "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)." *Jurnal Hukum Dan Bisnis (Selisik)*, 2020. https://doi.org/10.35814/selisik.v6i1.1699.

Official Journal Of European Union. "Artificial Intelligence Act," 2024.

Otoritas Jasa Keuangan. "Panduan Kode Etik Kecerdasan Buatan (Artificial Intelligence) Yang Bertanggung Jawab Dan Terpercaya Di Industri Teknologi Finansial," 2023.

Paminto, Saptaning Ruju. "Perlindungan Hukum Bagi Korban Pencurian Data Dan Informasi Pribadi Di Era Kejahatan Siber." *Jurnal Ilmu Hukum* 2, no. 2 (2025): 25–35. https://doi.org/https://doi.org/10.62017/syariah.

Rafasya, Raudhatul, Helfira Citra, and Engrina Fauzi. "Perlindungan Hukum Terhadap Konsumen Atas Pencurian Data Pribadi Dalam Transaksi Elektronik." *Jurnal Ilmu Sosial, Humaniora Dan Seni* 2, no. 2 (2023): 29–33. https://doi.org/10.62379/jishs.v2i2.1251.

Redaksi. "Menolak Lupa! Ini 10 Daftar Kasus Kebocoran Data Pribadi Di Indonesia," 2024.

Regita Citrazalzabila & Hudi Yusuf. "Pencurian Data Pribadi Di Internet Dari Sudut Pandang Kriminologi." *JICN: Jurnal Intelek Dan Cendikiawan Nusantara* 1, no. 2 (2024).

Rizki Kurniarullah, Muhammad, Talitha Nabila, Abdurrahman Khalidy, Vivi Juniarti Tan, Heni Widiyani, Ilmu Hukum Universitas Maritim Raja Ali Haji Abstrak, and Kata Kunci. "Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: Deepfake Pornografi Dan Pencurian Data Pribadi." *Jurnal Ilmiah Wahana Pendidikan* 10, no. 10 (2024): 534–47. https://doi.org/https://doi.org/10.5281/zenodo.11448813.

Romadian Amalia, Zaidatul Zulfa, Dewi Asri Puannandini. "Efektivitas Penerapan UU Perlindungan Data Pribadi Dalam Transaksi E-Commerce: Tinjauan Terhadap Keamanan Konsumen." *Jurnal Ilmu Hukum* 2, no. 2 (2025): 205–10. https://doi.org/https://doi.org/10.62017/syariah.

Sajjadi Mohammadabadi, Seyed Mahmoud, Burak Cem Kara, Can Eyupoglu, Can Uzay, Mehmet Serkan Tosun, and Oktay Karakuş. "A Survey of Large Language Models: Evolution, Architectures, Adaptation, Benchmarking, Applications, Challenges, and Societal Implications." *Electronics* 14, no. 18 (September 2025): 3580. https://doi.org/10.3390/electronics14183580.

Sakdiah, Halimatun, Nadiyah Geby, Theresa Ginting, Mayland Gea, and Neri Aisyah. "Korelasi Hak & Kewajiban Warga Negara & Negara Dalam Perlindungan Data Pribadi (Menyoroti Kasus Peretasan Data Nasional)" 3, no. 2 (2024): 1303–8. https://doi.org/http://dx.doi.org/10.57235/qistina.v3i2.4049.

Satrio Ulil Albab. "Perlindungan Hukum Terhadap Data Pribadi Nasabah Penyedia Jasa Pinjaman Bukan Bank Secara Online." *Ethics and Law Journal: Business and Notary* 2, no. 1 (January 2024): 176–82. https://doi.org/10.61292/eljbn.112.

Sepiyah. "Implikasi Hukum Terhadap Perlindungan Data Pribadi Di Era Digital." *Al-Balad: Jurnal Hukum Tata Negara Dan Politik Islam* 2, no. 1 (2022): 26–36.

Siber, Patroli. "Jumlah Laporan Polisi Yang Dibuat Masyarakat." Bareskrim Polri, 2025.

Sisilia, Klaudia, Yehizkia Adriaansz, Lucky Nurhadiyanto, Universitas Budi Luhur, Universitas Budi Luhur, Data Pribadi, Kejahatan Siber, Lifestyle Exposure, and Theft Identity. "Ancaman Risiko Keamanan Theft Identity Pada Aplikasi Berbasis Artificial Intelligence Dalam Perspektif Lifestyle Exposure Theory" 8, no. 2 (n.d.).

Stryker, Cole. "What Are LLMs?," 2024.

Taufik Hidayat Telaumbanua, Deasy Soekromo, Delasnova S. S. Lumintang. "Perlindungan Hukum Bagi Pengguna Media Sosial Terhadap Penyalahgunaan Data Pribadi Terkait Hak Privasi Menurut Hukum Positif." *Jurnal Fakultas Hukum Unsrat* 13, no. 01 (2024).

Verihubs. "Mengenal Cara Kerja AI: Dasar-Dasar Kecerdasan Buatan," 2024.

White, Kelle. "7 Ways AI Can Be Used by Hackers to Steal Personal Information," 2024.