

***The Digest:***

*Journal of Jurisprudence and Legisprudence*

Vol. 5 Issue 2 (2024) 231-262

DOI: <https://doi.org/10.15294/digest.v5i2.19941>

Available online since: January 23, 2025

**THE DIGEST** Journal of  
*Jurisprudence &  
Legisprudence*

# **Critically Reveal The Dimensions of Damage From Unauthorized Use of Personal Data**

(Study of Decision Number 78/Pid.Sus/2024/PN. Tng)

**Tegar Islami Putra** ✉

Faculty of Law, Universitas Negeri Semarang, Semarang, Indonesia  
[tegarislami44@students.unnes.ac.id](mailto:tegarislami44@students.unnes.ac.id)

**Nurul Fibrianti**

Faculty of Law, Universitas Negeri Semarang, Semarang, Indonesia  
[nurulfibrianti@mail.unnes.ac.id](mailto:nurulfibrianti@mail.unnes.ac.id)

**Adinda Zeranica Putri Fakhis**

Ahmad Ibrahim Kulliyah of Laws, Faculty of Law, International  
Islamic University Malaysia, Kuala Lumpur, Malaysia  
[a.zeranicafakhis@student.iium.edu.my](mailto:a.zeranicafakhis@student.iium.edu.my)

**Mohammad Raziq Fakhrullah**

Faculty of Civil Engineering, Universiti Teknologi Malaysia,  
Shah Alam, Malaysia  
[raziq2001@graduate.utm.my](mailto:raziq2001@graduate.utm.my)

✉ Corresponding email: [tegarislami44@students.unnes.ac.id](mailto:tegarislami44@students.unnes.ac.id)

## Abstract

Unauthorized use of personal data can cause harm to personal data subjects. In its mandate, Decision Number 78/Pid.Sus/2024/PN Tng provides a general outline of the potential harm that may occur to personal data subjects. However, the decision does not specifically explain the forms of loss and its impact on personal data subjects. This research critically discusses the forms of crimes causing harm and their impact on personal data subjects' damage due to unauthorized use of personal data in Decision Number 78/Pid.Sus/2024/PN Tng. The research employs the Library Research method, also known as Legal Research, which focuses on analyzing primary and secondary legal materials based on existing literature. The findings indicate that several general regulations in Indonesia address the crime of unauthorized use of personal data, including Law Number 24 of 2013, Law Number 1 of 2024, Law Number 14 of 2008, and Law Number 27 of 2022. Meanwhile, Decision Number 78/Pid.Sus/2024/PN Tng outlines the damage to personal data subjects resulting from unauthorized use of personal data, with this study revealing various impacts of damage both materially and non-materially.

## Keywords

*Critical Reveal; Damage; Unauthorized Use; Personal Data.*

## I. Introduction

Data protection can basically relate specifically to privacy as stated by Allan Westin who for the first time defined privacy as the right of individuals, groups or institutions to determine whether or not information about them will be communicated to other parties so that the definition put forward by Westin is called information privacy because it involves personal information.<sup>1</sup> The concept of data protection and cyber security is a form of effort made to protect user identity from various threats and legal access.<sup>2</sup> Indonesia as one of the countries based on law (*rechstaat*) and the rule of law, people really need legal protection to obtain legal certainty, and justice so that people feel prosperity.<sup>3</sup> In addition, in Indonesia, the Indonesian Internet Service Providers Association announced that the number of internet users in Indonesia in 2024 reach 221 million.<sup>4</sup>

The misuse of personal data can pose multiple dimensions of harm to the individuals affected. This is the impact of unauthorized use and disclosure of personal data. It is also a threat to the use of data in

---

<sup>1</sup> Tegar Islami Putra and Nurul Fibrianti, "Data Protection Impact Assessment Indicators In Protecting Consumer E-Commerce Platforms," *The Indonesian Journal of International Clinical Legal Education* 6, no. 1 (2024): 2.

<sup>2</sup> Abil Yositya Indah Mauliza, Rizky Dwi Salsabilla Machmudi, and Rachma Indrarini, "Pengaruh Perlindungan Data Dan Cyber Security Terhadap Tingkat Kepercayaan Menggunakan Fintech Masyarakat Di Surabaya," *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan* 1, no. 11 (2022): 2497.

<sup>3</sup> Tegar Islami Putra, "The Analysis of the Legal Protection of Ship's Crew in Sea Work Agreement in Indonesia," *Indonesian Journal of Advocacy and Legal Services* 5, no. 2 (2023): 185.

<sup>4</sup> Nurul Fibrianti et al., "Review of Child Consumer Protection in the Practice of Online Gambling Games Through the Gacha System," *The Indonesian Journal of International Clinical Legal Education* 6, no. 3 (2024): 429.

combination with.<sup>5</sup> In addition, according to Ida Siswanti as Head of The Legal Counseling Section of The Legal Bureau of the Secretariat General of The Ministry of Defence of The Republik of Indonesia explained, that human rights are limited by the other human right.<sup>6</sup> So in response to this, it is important to critically analyze the risk of unauthorized use of personal data. The emergence of changes in human life also creates new problems.<sup>7</sup>

This research will make one of the considerations in Decision Number 78/Pid.Sus/2024/PN Tng which clearly explains the forms of crime in the unauthorized use of personal data. The urgency of this research is given the rampant cases of leakage and misuse of personal data that occur in the world. So that the community, especially personal data protection practitioners such as personal data controllers, personal data processors, and data protection officers, need to understand it. Furthermore, the international dimension of data breaches emphasizes the interconnected nature of data protection challenges.<sup>8</sup>

Similar research has been conducted by Valiabhaneni in a study entitled Effects of Data Breaches on Internet of Things (IoT) Devices within the Proliferation of Daily-Life Integrated Devices and published in Engineering Technology Journal Vol.9 (7). Through the systematic

---

<sup>5</sup> Tegar Islami Putra and Nurul Fibrianti, "Threats and Legal Protection of Personal Data Combined in E-Commerce Transactions Based on Personal Data Protection Law in Indonesia," *Lambung Mangkurat Law Journal* 9, no. 1 (2024): 69.

<sup>6</sup> Tegar Islami Putra and Nurul Fibrianti, "Criminalization of Consumers for Criticism Given to Companies Through Cyberspace in Theoretical Studies," *Annual Review of Legal Studies* 1, no. 2 (2024): 183.

<sup>7</sup> Waspiyah Waspiyah et al., "Model Pelindungan Hukum Data Pribadi Di Era Digital Guna Menjamin Hak Warga Negara Atas Pelindungan Data Pribadi," *Syntax Literate ; Jurnal Ilmiah Indonesia* 8, no. 9 (2023): 5166.

<sup>8</sup> Tegar Islami Putra, Akbar Jihadul Islam, and Abdullah Mufti Abdul Rahman, "Integrating Islamic Laws into Indonesian Data Protection Laws: An Analysis of Regulatory Landscape and Ethical Considerations," *Contemporary Issues on Interfaith Law & Society* 4, no. 1 (2024): 89.

review method, this research produces findings that data leakage and privacy, denial-of-service attacks, and safety and security risks become damage to the occurrence of security breaches.<sup>9</sup>

Similar research has also been conducted by Khan and published in *Information & Management* Vol.58 (1). This research resulted in the finding that some damages from unauthorized use of personal data include confidentiality (adverse impact of data accessed outside of business needs), Availability (loss of access to data or data resources for an extended period of time), and Integrity (unauthorized or accidental manipulation of data while at rest, in transit, or in use regardless of the parties involved).<sup>10</sup>

Other similar research has also been conducted by Jung entitled *Extreme Data Breach Losses: An Alternative Approach to Estimating Probable Maximum Loss for Data Breach Risk* and published in the *North American Actuarial Journal* Vol.25 (4). This research proposes a measure of the maximum probable loss of data breach risk, which stands for the worst possible data breach loss, by using an alternative approach to estimating the potential loss level of an extreme event with one of the largest private databases for data breach risk. This research yields the findings that Cost estimation of the amount of loss due to a breach event (i.e. breached records) is important for both breached parties and cyber insurers, especially in third-party liability.<sup>11</sup>

However, there are limitations to the three studies mentioned above. The research determines Damage From Unauthorized Use Of Personal Data from the author's own views and research. Meanwhile, in

---

<sup>9</sup> Rohith Vallabhaneni, "Effects of Data Breaches on Internet of Things (IoT) Devices within the Proliferation of Daily-Life Integrated Devices," *Engineering and Technology Journal* 09, no. 07 (2024): 4440.

<sup>10</sup> Freeha Khan et al., "Data Breach Management: An Integrated Risk Model," *Information & Management* 58, no. 1 (January 2021): 9.

<sup>11</sup> Kwangmin Jung, "Extreme Data Breach Losses: An Alternative Approach to Estimating Probable Maximum Loss for Data Breach Risk," *North American Actuarial Journal* 25, no. 4 (October 2, 2021): 598.

the legal space in Indonesia, there has been a case of Unauthorized Use Of Personal Data decided by the judge through verdict number 78/Pid.Sus/2024/PN Tng which in its consideration determines the Damage From Unauthorized Use Of Personal Data. So that the purpose of this study is to determine the Damage From Unauthorized Use Of Personal Data which has been taken into consideration by the judge in making a decision in decision number 78/Pid.Sus/2024/PN Tng. In addition, the benefit of this research is to provide an overview to personal data controllers, personal data processors, personal data subjects, and legal practitioners to find out what damage from unauthorized use of personal data is.

Based on this background, the research question in this study include: (!) What are the forms of crime that harm the subject of personal data protection in the unauthorized use of personal data?; and (2) What are the form of personal data subject loss for unauthorized use of personal data in Decision Number 78/Pid.Sus/2024/PN Tng?

## II. Method

This scientific research uses one of the grand method sections, namely Library Research which is based on literature or literature. Based on the subject of study and the type of problem that exists, of the 3 (three) types of grand methods mentioned above, this research will use the Library Research method. Regarding this kind of research, it is also commonly called "Legal Research".<sup>12</sup> This kind of legal research does not recognize field research (field research) because what is studied is legal material so that it can be said to be library based, focusing on

---

<sup>12</sup> Soerjono Soekanto and Sri Mamudji, *Penelitian Hukum Normatif Tinjauan Singkat* (Jakarta: Rajawali Press, 2006): 66.

reading and analysis and analysis of the primary and secondary materials.<sup>13</sup>

### III. Forms of Crime that Harm the Subject of Personal Data Protection in the Unauthorized Use of Personal Data

In the Indonesian legal space, there are several articles that regulate forms of personal data crime. In Indonesian regulations, this form of crime is regulated in Article 77 jo. Article 94 of Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration, Article 95 of Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration, Article 95A of Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration, Article 32 jo. Article 48 of Law Number 1 Year 2024 on the Second Amendment to Law Number 11 Year 2008 on Electronic Information and Transactions, and Article 54 paragraph (1) of Law Number 14 Year 2008 on Public Information Disclosure. For the latest regulation related to the protection of personal data, the government has also enacted Law No. 27 of 2022 on the protection of personal data. These forms of crime are all actions that violate the principles of personal data protection.<sup>14</sup>

#### *Crimes of Manipulating, Accessing Databases, and Disseminating Population Data*

---

<sup>13</sup> Jhony Ibrahim, *Teori Dan Metodologi Penelitian Hukum Empiris* (Malang: Bayumedia Publishing, 2006): 98.

<sup>14</sup> *Ibid.*

The forms of data crime found in the Indonesian legal space are manipulating, accessing databases, and disseminating population data. This is as regulated in Law Number 23/2006 on Population Administration. These three things are regulated in different articles. In relation to manipulating population data, this also applies to those who order and/or facilitate this. This is regulated in Article 77 of the Population Administration Law on Population Administration which reads:

*"Every person is prohibited from ordering and/or facilitating and/or manipulating Population Data and/or Resident data elements."*

Furthermore, the criminal penalty for violating Article 77 of the Population Administration Law is regulated in Article 94 which reads:

*"Every person who orders and/or facilitates and/or manipulates Population Data and/or Resident data elements as referred to in Article 77 shall be punished with a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp75,000,000.00 (seventy-five million rupiah)."*

The second form of crime regulated in the Population Administration Law is related to accessing the population database. The crime of accessing the population database is regulated in Article 95 of the Population Administration Law which reads:

*"Any person who without right accesses the population database as referred to in Article 79 paragraph (1), Article 86 paragraph (1) shall be punished with imprisonment of 2 (two) years and/or a maximum fine of Rp 25,000,000.00 (twenty-five million rupiah)."*



The third form of crime regulated in the Population Administration Law is the dissemination of population data. This is as regulated in Article 95A of the Population Administration Law which reads:

*"Any person who without right disseminates Population Data as referred to in Article 79 paragraph (3) and Personal Data as referred to in Article 86 paragraph (1a) shall be punished with imprisonment of 2 (two) years and/or a maximum fine of Rp25,000,000.00 (twenty-five million rupiah)."*

The classification of population data referred to in the article above is explained in Article 58 paragraph (1) of the Population Administration Law, that Population Data consists of individual data and/or aggregate data of Residents. Furthermore, examples of the individual data in question, some of which are also types of personal data as stipulated in Law No. 27 of 2022 on Personal Data Protection, are as follows:

- a. Family Card Number;
- b. Identity Card Number;
- c. full name;
- d. gender;
- e. place of birth
- f. date/month/year of birth
- g. blood type
- h. religion/belief;
- i. marital status
- j. relationship status in the family;
- k. physical and/or mental disability
- l. last education;
- m. type of employment;
- n. birth mother's NIK;
- o. biological mother's name;

- p. father's NIK;*
- q. father's name*
- r. previous address*
- s. current address*
- t. ownership of birth certificate/birth recognition letter;*
- u. birth certificate number/birth recognition letter number;*
- v. ownership of marriage certificate/marriage book;*
- w. marriage certificate/marriage book number;*
- x. date of marriage;*
- y. ownership of a divorce certificate;*
- z. divorce certificate number/divorce certificate;*
- aa. date of divorce;*
- bb. fingerprints;*
- ā. iris;*
- aa. signature; and*
- ee. bb. other data elements that constitute a person's disgrace.*

### ***The Crime of Altering, Adding, Reducing, Transmitting, Damaging, Omitting, Moving, Hiding, and Moving or Transferring Data***

The next form of crime against data regulated in the Indonesian legal space is the crime of changing, adding, reducing, transmitting, damaging, eliminating, moving, hiding, and moving or transferring data. This is regulated in Law Number 1 Year 2024 on the Second Amendment to Law Number 11 Year 2008 on Electronic Information and Transactions (ITE Law). The forms of crimes against data in the ITE Law are regulated in Article 32 paragraphs (1) and (2) as follows:

- (1) Every person intentionally and without right or unlawfully by any means alters, adds, reduces, transmits, damages, eliminates, moves, hides Electronic Information and/or Electronic Documents belonging to another person or to the public.*

- (2) *Any Person intentionally and without right or unlawfully by any means moves or transfers Electronic Information and/or Electronic Documents to the Electronic System of another unauthorized person.*

In the ITE Law, the definition of electronic information is explained in Article 1 number 1, namely:

*“Electronic Information is one or a set of electronic data, including but not limited to writings, sounds, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or the like, letters, signs, numbers, Access Codes, symbols, or perforations that have been processed which have meaning or can be understood by people who are able to understand them.”*

Meanwhile, the definition of electronic documents in the ITE Law is explained in Article 1 number 4 which reads:

*“Electronic Information is one or a set of electronic data, including but not limited to writings, sounds, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail (electronic maill, telegram, telex, telecopy or the like, letters, signs, numbers, access codes, symbols, or perforations that have been processed which have meaning or can be understood by a person capable of understanding them.”*

In the event of a violation of Article 32 paragraphs (1) and (2) of the ITE Law as mentioned, there are criminal threats stipulated in Article 48 as follows:

- (1) *Every person who fulfills the elements as referred to in Article 32 paragraph (1) shall be punished with a maximum imprisonment of 8 (eight) years and/or a maximum fine of Rp2,000,000,000.00 (two billion rupiah).*

- (2) *Every person who fulfills the elements as referred to in Article 32 paragraph (2) shall be punished with a maximum imprisonment of 9 (nine) years and/or a maximum fine of Rp3,000,000,000.00 (three billion rupiah).*

***Crimes of Acquisition/Collection, Disclosure, and Use of Personal Data***

The next form of crime against data that is regulated in the legal space in Indonesia is the prohibition for someone who intentionally and unlawfully Obtains/Collects, Discloses, and Uses Personal Data. This is as stipulated in Law Number 27 Year 2022 on Personal Data Protection. The prohibition is regulated in Article 65 paragraphs (1), (2), and (3) which reads:

- (1) *Every Person is prohibited from unlawfully obtaining or collecting Personal Data that does not belong to him/her with the intention to benefit himself/herself or others which may result in harm to the Personal Data Subject.*
- (2) *Any Person shall be prohibited from unlawfully disclosing Personal Data that does not belong to him/her.*
- (3) *Every Person shall be prohibited from unlawfully using Personal Data that does not belong to them.*

Furthermore, in the event of violation of Article 65 paragraph (1), (2), and (3) of the Personal Data Protection Law, there are criminal penalties stipulated in Article 67 paragraph (1), (2), and (3) as follows:

- (1) *Any Person who intentionally and unlawfully obtains or collects Personal Data that does not belong to him/her with the intention to benefit himself/herself or another person which may result in the loss of the Personal Data Subject as referred to in Article 65 paragraph (1) shall be punished with a maximum imprisonment of 5 (five) years and/or a maximum fine of Rp5,000,000,000.00 (five billion rupiah).*
- (2) *Any Person who intentionally and unlawfully discloses Personal Data that does not belong to him as referred to in Article 65 paragraph (2)*

- shall be punished with a maximum imprisonment of 4 (four) years and/or a maximum fine of Rp4,000,000,000.00 (four billion rupiah).*
- (3) *Every Person who intentionally and unlawfully uses Personal Data that does not belong to him as referred to in Article 65 paragraph (3) shall be punished with a maximum imprisonment of 5 (five) years and/or a maximum fine of Rp5.000.000.000,00 (five billion rupiah).*

The types of personal data referred to in Law Number 27 Year 2022 are regulated in Article 4 paragraph (1) which provides a classification into specific and general personal data. Furthermore, paragraph (2) provides examples of the personal data in question. The specific personal data are:

- a. health data and information;*
- b. biometric data;*
- c. genetic data*
- d. crime records;*
- e. child data*
- f. personal information data; and/or*
- g. other data in accordance with the provisions of laws and regulations.*

Furthermore, Article 4 paragraph (2) provides examples of general personal data. The general personal data are:

- a. full name;*
- b. gender*
- c. citizenship*
- d. religion*
- e. marital status; and/or*
- f. personal data combined to identify a person.*

## IV. Personal Data Subject's Damage for Unauthorized Use of Personal Data in Decision Number 78/Pid.Sus/2024/PN Tng

One of the judges' considerations in Decision Number 78/Pid.Sus/2024/PN Tng states that based on the considerations, the element of intentionally unlawfully using personal data that does not belong to him as referred to in Article 65 paragraph (3) must be declared fulfilled. The element referred to in this case is the element of intentionally and unlawfully obtaining or collecting personal data that does not belong to him with the intention of benefiting himself or others which may result in harm to the personal data subject. Decision Number 78/Pid.Sus/2024/PN Tng also explains that in terms of losses, the owner of personal data may experience losses to the subject of personal data both directly and indirectly such as financial crimes such as extortion, fraud, loan applications, online applications (pinjol), illegal money transactions, and claiming to be someone else to get social assistance, health services, employment programs, spam, and phishing via email, messenger, telephone, and others. However, Decision Number 78/Pid.Sus/2024/PN Tng does not explain in more detail the form of harm to the personal data subject's for unauthorized use of personal data. Whatever it is, the function of law as protector of various human interests must continue to be carried out, both in normal and peaceful situations, as well as when law violation occurs.<sup>15</sup>

---

<sup>15</sup> Asmarani Ramli et al., "Applying In Dubio Pro Natura in Environmental Crime Cases: Legal Perspectives in Indonesia," *The Indonesian Journal of International Clinical Legal Education* 5, no. 4 (December 28, 2023): 430.

### *Extortion*

The first direct or indirect loss of personal data subject as referred to in Decision Number 78/Pid.Sus/2024/PN Tng is extortion. This crime not only harms the victim financially but also causes deep psychological trauma.<sup>16</sup> Extortion has a very serious and complex impact on its victims, ranging from psychological impacts such as trauma, prolonged stress, and loss of security, to financial impacts in the form of material losses from the extorted assets.

Perbuatan pemerasan merupakan masalah yang mempengaruhi seluruh bangsa, membahayakan pencapaian tujuan negara dan merugikan masyarakat Indonesia, mengingat potensi dampaknya yang merugikan masyarakat.<sup>17</sup> Extortion is a problem that affects the entire nation, jeopardizing the achievement of state goals and harming the Indonesian people, given its potential detrimental impact on society. Extortion is basically an unlawful act of forcing someone with violence or theft preceded by violence or threats of violence, either taken by the suspect himself or the delivery of goods by the victim.<sup>18</sup> Victims also often experience social impacts such as reputational damage and social isolation, as well as physical impacts that include stress-induced health problems and a reduced immune system. In the long term, extortion can cause permanent changes in the victim's life, including difficulty building trust and ongoing trauma. In extortion, the perpetrator uses intimidation in the form of acts of violence, while threatening itself is

---

<sup>16</sup> Rini Andriani Butar, "Sanksi Pidana Untuk Pemerasan Dan Ancaman Online Cybersex: Analisis Putusan Nomor: 229/Pid. Sus/2021/PN. Prp Dalam Perspektif Hukum Islam," *Indonesian Journal of Humanities and Social Sciences* 5, no. 3 (2024): 1108.

<sup>17</sup> Karina Hasiyanni Manurung and Kayus Kayowuan Lewoleba, "Penerapan Sanksi Etika Profesi Terhadap Anggota Polisi Yang Melakukan Pemerasan," *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial* 1, no. 4 (2023): 136.

<sup>18</sup> Hafied Cangara, *Pengantar Ilmu Komunikasi* (Jakarta: PT RajaGrafindo Persada, 2002): 23.

more likely to use defamation or provide verbal or written arguments intended to deprive material and non-material rights.<sup>19</sup>

### *Fraud*

The second direct or indirect loss of personal data subject as intended in Decision Number 78/Pid.Sus/2024/PN Tng is fraud. Lack of understanding of the increasingly sophisticated fraud modes makes a person vulnerable to being cheated by irresponsible parties. Fraud against personal data is carried out by people who understand Information and Technology (IT) and is referred to as a form of cyber crime. Unlike computer crime which is usually carried out by IT professionals, by spreading viruses and computer hacking.<sup>20</sup>

The fraud mode that is quite rampant at this time is the spread of phishing links on behalf of certain organizations/groups that provide great benefits and offer attractive prizes to us if we click on the link. However, when the link is opened, the owner of personal data will be sent malware or viruses, then his personal data is hacked. Thus, everyone needs to equip themselves by finding out regularly about the fraud modes that are currently prevalent. However, when the link is opened, the owner of personal data will be sent malware or viruses, then his personal data is hacked. Thus, everyone needs to equip themselves by finding out regularly about the fraud modes that are currently prevalent.<sup>21</sup>

---

<sup>19</sup> Adami Chazawi, *Kejahatan Terhadap Harta Benda* (Malang: Bayu Media, 2006): 52.

<sup>20</sup> Fendi Tri Cahyono, "STRUCTURAL EQUATION MODELING UNTUK MENGUKUR FAKTOR-FAKTOR MOTIF KRIMINALITAS (Studi Kasus: Kepolisian Resor Kota Yogyakarta)" (UNIVERSITAS GADJAH MADA, 2017): 7.

<sup>21</sup> Moody R. Syailendra and Samantha Elizabeth Fitzgerald, "Sosialisasi Perlindungan Data Pribadi Bagi Masyarakat Kabupaten Indramayu," *Jurnal Serina Abdimas* 1, no. 1 (2023): 162.



As a simple example, the implementation of the agreement in Peer to Peer Lending sees that a debtor or loan recipient is proven by using an identity card such as KTP, SIM, or other identity cards in the form of documents or photos. So that this allows fraud to occur in the Peer to Peer Lending agreement, such as on the debtor's side there is a fear of personal data fraud, manipulating identity by using another identity and when viewed from the creditor's side there is a fear of leaking personal data on the grounds of non-fulfillment of achievements.<sup>22</sup>

The discussion is written to interpret and describe the significance of your findings in light of what was already known about the issues being investigated, and to explain any new understanding or insights about the problem after you have taken the findings into consideration. It should connect to the introduction by way of the research questions or hypotheses you posed and the literature you reviewed, but it does not simply repeat or rearrange the introduction; this section should always explain how your study has moved the reader's understanding of the research problem forward from where you left them at the end of the introduction.

### *Loan Application & Online Loan Application*

The first direct or indirect loss of personal data subject as intended in Decision Number 78/Pid.Sus/2024/PN Tng is loan application & online loan application. The provision of interest on online loans, which has not been regulated in Indonesian laws and regulations, as well as the practice of online loans that do not transparently disclose the interest, shows that there is a difference in the position of the parties, which leads to vulnerable losses for loan recipients as consumers.<sup>23</sup> The recipient of

---

<sup>22</sup> Ariza Umami et al, "Juridical Review the Validity of the Agreement on Peer," *Otentik's Jurnal Hukum Kenotariatan (Vol 5 No.1, Januari 2023)* 5, no. 1 (2023): 12..

<sup>23</sup> Sidharta, *Aspek Hukum Ekonomi Dan Bisnis* (Jakarta: Prenadamedia, 2018): 24.

the loan becomes easily defaulted due to the absence of awareness regarding the amount of interest. When defaulting, it will lead to actions that injure the rights of the loan recipient, which actually occurs due to ignorance due to the lack of transparency from the online loan service provider, including with regard to interest transparency.<sup>24</sup>

Illegal online loans are an illustration of the simplification of the financing system that is facilitated by quite attractive offers without complicated bureaucracy, which turns out to be a time bomb for the community because it ensnares various complex problems in it. By knowing a person's personal data very specifically, this can be used to apply for a loan. Online loan scams that cause a lot of harm to the community.<sup>25</sup> There are many impacts of online loans on society that result in losses.<sup>26</sup>

### *Illegal Money Transactions*

The first direct or indirect loss of personal data subject as intended in Decision Number 78/Pid.Sus/2024/PN Tng is illegal money transactions. The illegal money transaction referred to in this case is the implementation of financial transactions that are carried out illegally. An example of a case in this regard is the misuse of personal data on an online loan application, where a person suddenly receives a transfer of funds to his account without ever applying for a loan. The victim then receives threats via email to return the funds along with interest within

---

<sup>24</sup> Kevin Septian Anugrah Perdana and Hariyo Sulistiyantoro, "Urgensi Transparansi Besaran Bunga Dalam Perjanjian Pinjaman Online," *Jurnal Ilmiah Wahana Pendidikan* 9, no. 19 (2023): 432.

<sup>25</sup> Sri Lestari Poernomo, "PERLINDUNGAN HUKUM KONSUMEN TERHADAP PRAKTIK TEKNOLOGI FINANSIAL ILEGAL DALAM BENTUK PINJAMAN ONLINE ILEGAL," *Mimbar Keadilan* 15, no. 1 (2022): 134.

<sup>26</sup> Darmi Wati and Triyana Syahfitri, "Dampak Pinjaman Online Bagi Masyarakat," *Community Development Journal: Jurnal Pengabdian Masyarakat* 2, no. 3 (2022): 1182.

a certain time limit. Even though the victim had tried to clarify to the service provider that he had never applied for a loan, the application still forced the victim to pay. After the victim paid the requested amount, the problem did not stop - a few months later the victim received a similar bill from the same company but changed its name.<sup>27</sup> Contoh kasus lain adalah penggunaan teknologi AI deepfake kemudian banyak menimbulkan permasalahan seperti disalahgunakan untuk mendapatkan pinjaman online yang hanya membutuhkan data pribadi seperti Kartu Tanda Penduduk (KTP) dan foto selfie (swafoto) sambil memegang KTP,<sup>28</sup> Another case example is the use of deepfake AI technology, which then causes many problems such as being misused to obtain online loans that only require personal data such as an Identity Card (KTP) and a selfie (selfie) while holding the KTP, Another example of the losses that can be experienced by personal data subjects in terms of illegal money transactions is in the case of application-based lending, fintech lending companies can use consumers' personal data without the permission or knowledge of consumers.<sup>29</sup> In response to this, the process of monitoring and evaluating performance is a crucial step to ensure the sustainability and effectiveness of the business.<sup>30</sup>

---

<sup>27</sup> Hafsha Amalia Hasnan, "Perlindungan Hukum Penyalahgunaan Artificial Intelligence Deepfake Pada Layanan Pinjaman Online" (Universitas Muhammadiyah Surakarta, 2022): 3.

<sup>28</sup> *Ibid.*

<sup>29</sup> Erwin Asmadi, "PENYELEWENGAN DATA PRIBADI DALAM PEMANFAATAN APLIKASI FINANCIALTEKNOLOGI(PINJAMAN ONLINE)," *Seminar Nasional Hukum, Sosial, Dan Ekonomi* 2, no. 1 (2022): 138.

<sup>30</sup> Slamet Sumarto et al., "Unlocking Village Potential: Empowering Tanuharjo Officials to Boost Revenue through Village-Owned Enterprises," *Jurnal Pengabdian Hukum Indonesia* 7, no. 1 (2024): 8.

*Impersonation of Others to Obtain Social Assistance, Health Services, Employment Programs, Spam, and Phishing*

The first direct or indirect personal data subject harms as intended in Decision No. 78/Pid.Sus/2024/PN Tng are illegal money transactions of recognition as another person to obtain social assistance, health services, employment programs, spam, and phishing. Basically, personal data includes any information that can be used to identify or contact a specific individual, whether the information is collected directly or indirectly through electronic and/or non-electronic methods.<sup>31</sup> With the knowledge of a person's identity in the form of personal data by other people, these other people can use it to identify. This is because personal data will refer to any information that can directly or indirectly identify a person.<sup>32</sup>

In terms of recognition to obtain social assistance, it will be related to the validity of data on workers receiving social assistance or salary subsidies from the government, referring to the rules in Permenaker No. 14 of 2020 concerning Guidelines for Providing Government Assistance in the Form of Salary / Wage Subsidies for Workers / Laborers.<sup>33</sup> The Permenaker, which came into force on August 14, 2020, stipulates the recipient requirements and the method of providing BLT as stated in Article 3 which states: (1) Government assistance in the form of Salary/Wage subsidies is given to Workers/Laborers; (2) Workers/Laborers as referred to in paragraph (1) must meet the following requirements: (a) Indonesian citizen as evidenced by the

---

<sup>31</sup> Kadek Rima Anggen Suari and I Made Sarjana, "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia," *Jurnal Analisis Hukum* 6, no. 1 (2023): 132..

<sup>32</sup> D. F. F Mahira, E Yofita, and L. N Azizah, "Consumer Protection System (CPS): Sistem Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept," *Jurnal Legislatif* 3, no. 2 (2020): 287.

<sup>33</sup> Hartini Retnaningsih, "Bantuan Sosial Bagi Pekerja Di Tengah Pandemi Covid-19: Sebuah Analisis Terhadap Kebijakan Sosial Pemerintah," *Aspirasi: Jurnal Masalah-Masalah Sosial* 11, no. 2 (2020): 222.

population identification number; (b) registered as an active participant of the BPJS Employment social security program as evidenced by the membership card number; (c) Salary/Wage recipient Worker/Laborer; (d) membership until June 2020; (e) active participants of the employment social security program who pay contributions with the amount of contributions calculated based on Salary/Wage below Rp5.000,000.00 (five million rupiah) according to the last Salary/Wage reported by the employer to BPJS Ketenagakerjaan and recorded at BPJS Ketenagakerjaan; and (f) have an active bank account.<sup>34</sup> Through some of the data collected, it can be used to identify some other data that includes a person's personal data based on the mandate of Article 4 paragraphs (2) and (3) of Law Number 27 of 2022.

Furthermore, in terms of health service utilization, there is a system called e-prescribing. Electronic prescribing system (e-prescribing) is a prescribing system using software designed to facilitate drug prescription services starting from the prescription writing stage (prescribing), reading the prescription for the dispensing process (transcribing), the preparation stage until the delivery of the prescription by the officer (dispensing), the process of using the drug (administration stage) and the monitoring process.<sup>35</sup> This also affects the patient's personal data, which of course is not only contained in the patient's electronic medical record but also stored in the third party electronic prescription system, namely the pharmacy. In the electronic prescription process, the patient's personal data included is almost the same as that contained in the medical record or sourced from the

---

<sup>34</sup> *Ibid.*

<sup>35</sup> Annie Hahn and Annesha Lovett, "Electronic Prescribing: An Examination of Cost Effectiveness, Clinician Adoption and Limitations," *Universal Journal of Clinical Medicine* 2, no. 1 (January 2014): 18.

medical record.<sup>36</sup> Medical records are a collection of information that includes patient identity, examination results, types of treatment given, medical procedures performed, and other services that have been provided to patients.<sup>37</sup> Through some of the data collected, there is data that is directly personal data as mandated by Law Number 27 of 2022, such as health data and information, genetic data, full name, and gender.

Furthermore, in terms of workforce program utilization, an example is found in the implementation of the staffing management information system at the Staffing and Human Resources Development Agency of Bombana.<sup>38</sup> In implementing the management information system policy, it is necessary to evaluate and select the right management information system that has a high level of security. In addition, the readiness of users or operators who input data in the online academic information system also needs to be considered. Leaders must also be consistent with the policies delivered so that there are no changes in information in the information system.<sup>39</sup>

Overall, there are three approaches that can be taken to minimize the misuse of information technology, namely (1) Legal approach, with the availability of national positive legal instruments related to the use of information technology will provide a guarantee of certainty and as a basis for law enforcement in the event of a violation; (2) Technological

---

<sup>36</sup> Lalu Anugrah Nugraha et al., "Perlindungan Hukum Rumah Sakit Atas Penggunaan Data Pasien Dalam Peresepan Elektronik," *Unizar Law Review* 6, no. 2 (December 20, 2023): 203.

<sup>37</sup> Antonius Dewanto Purnomo, "KAJIAN EMPIRIK PERMASALAHAN PENERAPAN HUKUM PERSELISIHAN PERBURUHAN, PEMUTUSAN HUBUNGAN KERJA DAN PERLINDUNGAN PRIVASI DATA PRIBADI," *Blantika: Multidisciplinary Jurnal* 2, no. 6 (2024): 672.

<sup>38</sup> Siti Hapsah Pahira, Rio Rinaldy, and Evi Lativah, "Perspektif Hukum Mengenai Penyalahgunaan Data Pribadi Pada Sistem Informasi Manajemen," *Jurnal Sosial Teknologi* 3, no. 7 (2023): 622..

<sup>39</sup> *Ibid.*

security approach, in this case the technological approach is absolutely necessary, with a sophisticated technological security system that can close holes that can be used for misuse; and (3) Socio-cultural-ethical approach, this approach is very important because it provides understanding from a socio-cultural point of view so that people understand that information technology has very high effectiveness in global trade.<sup>40</sup> Meanwhile, efforts to overcome misuse of management information systems can be done in several ways, namely (1) Implementation of clear and strict policies and procedures to protect company assets or assets from all forms of misuse, and ensure the availability of accurate company accounting information; (2) Evaluation and selection of management information systems that are appropriate and have a high level of security; (3) Training and socialization to company employees regarding established policies and procedures, as well as the importance of maintaining the confidentiality of personal data and company information; (4) Implementation of information security technology, such as firewalls, antivirus, and data encryption, to prevent unauthorized access to management information systems; and (5) Regulation against theft of personal data as a misuse of communication and information technology.<sup>41</sup>

Furthermore, in the case of spam and phishing crimes, a person can commit these crimes when they already know the personal data of their potential victims. In the case of phishing, where customer data is stolen by luring customers to provide their personal information through internet banking channels without realizing it, which ultimately results in the loss of customer money without using a credit card or debit card.<sup>42</sup> As an example scenario, a phisher who knows the

---

<sup>40</sup> *Ibid.*

<sup>41</sup> *Ibid.*

<sup>42</sup> Tegar Islami Putra, “Juridical Analysis of The Application of Local Currency Settlement Between Indonesia and China in Business Transactions,” *Journal of Private and Commercial Law* 7, no. 2 (2023): 28.

victim's health data, full name, and cell phone number (belonging to the victim) can pose as a staff member of a hospital or clinic where the victim has been treated. The perpetrator contacts the victim via SMS or WhatsApp message, claiming that the results of a health check-up show the need for further action regarding a certain condition, such as heart disease. The perpetrator offers a special discount for check-up services and asks the victim to click on a link that redirects to a fake website that resembles an official hospital page. On the site, the victim is asked to fill in additional data, such as financial information or personal identity. If the victim is deceived, the data can be used by the perpetrator for identity theft or financial fraud. In addition, with the victim's personal data known, the perpetrator can also send spam (unsolicited or unwanted messages) via email address or cell phone number to the victim. For this reason, people should be careful and pay attention to signs of phishing such as unknown emails or messages, unknown links, or requests for personal information that is not usually given.<sup>43</sup>

## V. Conclusion

Law Number 24 of 2013, Law Number 1 of 2024, Law Number 14 of 2008, and Law Number 27 of 2022 regulate the crime of unauthorized use of personal data. The forms of crime regulated in these laws include manipulating population data, accessing population data, disseminating population data, altering, adding, reducing, transmitting, damaging, removing, moving, hiding electronic information, transferring or moving electronic information and/or electronic documents to unauthorized third-party electronic systems, disclosing personal data

---

<sup>43</sup> Ananta Fadli Sutarl and Shelly Kurniawan, "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi Dalam Menanggulangi Phising Di Indonesia," *INNOVATIVE: Journal Of Social Science Research* 3, no. 2 (2020): 4210.



beyond what is required for public agency access, unlawfully obtaining or collecting personal data, unlawfully disclosing personal data, and unlawfully using personal data. Specifically, Decision Number 78/Pid.Sus/2024/PN Tng discusses the damage to personal data subjects caused by the unauthorized use of personal data, with this study revealing various material and non-material impacts of such damage.

## VI. References

- Anggen Suari, Kadek Rima, and I Made Sarjana. "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia." *Jurnal Analisis Hukum* 6, no. 1 (2023): 132–142. <https://doi.org/10.38043/jah.v6i1.4484>.
- Ariza Umami et al. "Juridical Review the Validity of the Agreement on Peer." *Otentik's Jurnal Hukum Kenotariatan (Vol 5 No.1, Januari 2023)* 5, no. 1 (2023): 1-22. <https://doi.org/doi.org/10.35814/otentik.v5i1.4583>.
- Asmadi, Erwin. "PENYELEWENGAN DATA PRIBADI DALAM PEMANFAATAN APLIKASI FINANCIALTEKNOLOGI(PINJAMAN ONLINE)." *Seminar Nasional Hukum, Sosial, Dan Ekonomi* 2, no. 1 (2022): 135-145.
- Butar, Rini Andriani. "Sanksi Pidana Untuk Pemerasan Dan Ancaman Online Cybersex: Analisis Putusan Nomor: 229/Pid. Sus/2021/PN. Prp Dalam Perspektif Hukum Islam." *Indonesian Journal of Humanities and Social Sciences* 5, no. 3 (2024): 1107-1120. <https://doi.org/https://doi.org/10.33367/ijhass.v5i3.5876>.
- Cahyono, Fendi Tri. "STRUCTURAL EQUATION MODELING UNTUK MENGUKUR FAKTOR-FAKTOR MOTIF

- KRIMINALITAS (Studi Kasus: Kepolisian Resor Kota Yogyakarta).” UNIVERSITAS GADJAH MADA, 2017.
- Cangara, Hafied. *Pengantar Ilmu Komunikasi*. Jakarta: PT RajaGrafindo Persada, 2002.
- Chazawi, Adami. *Kejahatan Terhadap Harta Benda*. Malang: Bayu Media, 2006.
- Fibrianti, Nurul, Tri Andari Dahlan, Rahayu Fery Anitasari, Niken Diah Paramita, and Tegar Islami Putra. “Review of Child Consumer Protection in the Practice of Online Gambling Games Through the Gacha System.” *The Indonesian Journal of International Clinical Legal Education* 6, no. 3 (2024): 427-452. <https://doi.org/doi.org/10.15294/ijicle.v6i3.13198>.
- Hahn, Annie, and Annesha Lovett. “Electronic Prescribing: An Examination of Cost Effectiveness, Clinician Adoption and Limitations.” *Universal Journal of Clinical Medicine* 2, no. 1 (January 2014): 1-24. <https://doi.org/10.13189/ujcm.2014.020101>.
- Hapsah Pahira, Siti, Rio Rinaldy, and Evi Lativah. “Perspektif Hukum Mengenai Penyalahgunaan Data Pribadi Pada Sistem Informasi Manajemen.” *Jurnal Sosial Teknologi* 3, no. 7 (2023): 620-626. <https://doi.org/10.59188/jurnalsostech.v3i7.890>.
- Hasnan, Hafsha Amalia. “Perlindungan Hukum Penyalahgunaan Artificial Intelligence Deepfake Pada Layanan Pinjaman Online.” Universitas Muhammdaiyah Surakarta, 2022.
- Ibrahim, Jhony. *Teori Dan Metodologi Penelitian Hukum Empiris*. Malang: Bayumedia Publishing, 2006.
- Jung, Kwangmin. “Extreme Data Breach Losses: An Alternative Approach to Estimating Probable Maximum Loss for Data Breach Risk.” *North American Actuarial Journal* 25, no. 4 (October 2, 2021): 580-603.

<https://doi.org/10.1080/10920277.2021.1919145>.

Khan, Freeha, Jung Hwan Kim, Lars Mathiassen, and Robin Moore. "DATA BREACH MANAGEMENT: AN INTEGRATED RISK MODEL." *Information & Management* 58, no. 1 (January 2021): 1-12. <https://doi.org/10.1016/j.im.2020.103392>.

Lalu Anugrah Nugraha, Sutarno Sutarno, Ninis Nugraheni, and Andika Persada Putra. "Perlindungan Hukum Rumah Sakit Atas Penggunaan Data Pasien Dalam Pereseapan Elektronik." *Unizar Law Review* 6, no. 2 (December 20, 2023): 199-208. <https://doi.org/10.36679/ulr.v6i2.45>.

Mahira, D. F. F, E Yofita, and L. N Azizah. "Consumer Protection System (CPS): Sistem Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept." *Jurnal Legislatif* 3, no. 2 (2020): 287-302. <https://doi.org/doi.org/10.20956/jl.v3i2.10472>.

Manurung, Karina Hasiyanni, and Kayus Kayowuan Lewoleba. "Penerapan Sanksi Etika Profesi Terhadap Anggota Polisi Yang Melakukan Pemerasan." *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial* 1, no. 4 (2023): 134-141. <https://doi.org/https://doi.org/10.5281/zenodo.10214304>.

Mauliza, Abil Yositya Indah, Rizky Dwi Salsabilla Machmudi, and Rachma Indrarini. "Pengaruh Perlindungan Data Dan Cyber Security Terhadap Tingkat Kepercayaan Menggunakan Fintech Masyarakat Di Surabaya." *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan* 1, no. 11 (2022): 2497-2516. <https://doi.org/10.54443/sibatik.v1i11.395>.

Perdana, Kevin Septian Anugrah, and Hariyo Sulistiyantoro. "Urgensi Transparansi Besaran Bunga Dalam Perjanjian Pinjaman Online." *Jurnal Ilmiah Wahana Pendidikan* 9, no. 19 (2023): 429-436.

Poernomo, Sri Lestari. "PERLINDUNGAN HUKUM KONSUMEN

- TERHADAP PRAKTIK TEKNOLOGI FINANSIAL ILEGAL DALAM BENTUK PINJAMAN ONLINE ILEGAL.” *Mimbar Keadilan* 15, no. 1 (2022):134-148. <https://doi.org/https://doi.org/10.24853/justit.9.2.100-107>.
- Purnomo, Antonius Dewanto. “KAJIAN EMPIRIK PERMASALAHAN PENERAPAN HUKUM PERSELISIHAN PERBURUHAN, PEMUTUSAN HUBUNGAN KERJA DAN PERLINDUNGAN PRIVASI DATA PRIBADI.” *Blantika: Multidisciplinary Jurnal* 2, no. 6 (2024): 667-674. <https://doi.org/doi.org/10.57096/blantika.v2i7.162>.
- Putra, Tegar Islami. “Juridical Analysis of The Application of Local Currency Settlement Between Indonesia and China in Business Transactions.” *Journal of Private and Commercial Law* 7, no. 2 (2023): 13–34.
- . “The Analysis of the Legal Protection of Ship’s Crew in Sea Work Agreement in Indonesia.” *Indonesian Journal of Advocacy and Legal Services* 5, no. 2 (2023): 181–206. <https://doi.org/10.15294/ijals.v5i2.75367>.
- Putra, Tegar Islami, and Nurul Fibrianti. “Criminalization of Consumers for Criticism Given to Companies Through Cyberspace in Theoretical Studies.” *Annual Review of Legal Studies* 1, no. 2 (2024): 179-204.
- . “Data Protection Impact Assessment Indicators In Protecting Consumer E-Commerce Platforms.” *The Indonesian Journal of International Clinical Legal Education* 6, no. 1 (2024): 1-22.
- . “Threats and Legal Protection of Personal Data Combined in E-Commerce Transactions Based on Personal Data Protection Law in Indonesia.” *Lambung Mangkurat Law Journal* 9, no. 1 (2024): 64–74. <https://doi.org/10.32801/lamlaj.v9i1.438>.

- Putra, Tegar Islami, Akbar Jihadul Islam, and Abdullah Mufti Abdul Rahman. "Integrating Islamic Laws into Indonesian Data Protection Laws: An Analysis of Regulatory Landscape and Ethical Considerations." *Contemporary Issues on Interfaith Law & Society* 4, no. 1 (2024): 85–118. <https://doi.org/doi.org/10.15294/ciils.v3i1.78690>.
- R. Syailendra, Moody, and Samantha Elizabeth Fitzgerald. "Sosialisasi Perlindungan Data Pribadi Bagi Masyarakat Kabupaten Indramayu." *Jurnal Serina Abdimas* 1, no. 1 (2023): 157-165. <https://doi.org/10.24912/jsa.v1i1.23845>.
- Ramli, Asmarani, Tegar Islami Putra, Natasya Fitri Dewanti, Salisa Widyaning Kinasih, and Ridwan Arifin. "Applying In Dubio Pro Natura in Environmental Crime Cases: Legal Perspectives in Indonesia." *The Indonesian Journal of International Clinical Legal Education* 5, no. 4 (December 28, 2023): 409-444. <https://doi.org/10.15294/ijicle.v5i4.76091>.
- Retnaningsih, Hartini. "Bantuan Sosial Bagi Pekerja Di Tengah Pandemi Covid-19: Sebuah Analisis Terhadap Kebijakan Sosial Pemerintah." *Aspirasi: Jurnal Masalah-Masalah Sosial* 11, no. 2 (2020): 215-227: 222. <https://doi.org/10.46807/aspirasi.v11i2.1756>.
- Sidharta. *Aspek Hukum Ekonomi Dan Bisnis*. Jakarta: Prenadamedia, 2018.
- Soekanto, Soerjono, and Sri Mamudji. *Penelitian Hukum Normatif Tinjauan Singkat*. Jakarta: Rajawali Press, 2006.
- Sumarto, Slamet, Martitah Martitah, Natal Kristiono, Arif Hidayat, and Tegar Islami Putra. "Unlocking Village Potential: Empowering Tanuharjo Officials to Boost Revenue through Village-Owned Enterprises." *Jurnal Pengabdian Hukum Indonesia* 7, no. 1 (2024): 1-16.

- Sutarl, Ananta Fadli, and Shelly Kurniawan. "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi Dalam Menanggulangi Phising Di Indonesia." *INNOVATIVE: Journal Of Social Science Research* 3, no. 2 (2020): 4208-4221. <https://doi.org/10.5040/9781635577068-0537>.
- Vallabhaneni, Rohith. "Effects of Data Breaches on Internet of Things (IoT) Devices within the Proliferation of Daily-Life Integrated Devices." *Engineering and Technology Journal* 09, no. 07 (2024): 4439-4442. <https://doi.org/10.47191/etj/v9i07.13>.
- Waspiah, Waspiah, Noveria Sekar S, Ammirah Lies S, Tegar Islami Putra, Setyaning Wida N, and Salisa Widyaning K. "Model Pelindungan Hukum Data Pribadi Di Era Digital Guna Menjamin Hak Warga Negara Atas Pelindungan Data Pribadi." *Syntax Literate ; Jurnal Ilmiah Indonesia* 8, no. 9 (2023): 5165–5179. <https://doi.org/10.36418/syntax-literate.v8i9.13662>.
- Wati, Darmi, and Triyana Syahfitri. "Dampak Pinjaman Online Bagi Masyarakat." *Community Development Journal: Jurnal Pengabdian Masyarakat* 2, no. 3 (2022): 1181-1186. <https://doi.org/10.31004/cdj.v2i3.2950>.
- Medis." *Jurnal Hukum Pelita* 4, no. 1 (2023): 67–78. <https://doi.org/10.37366/jh.v4i1.2378>.
- Zaman, Rutabuz. "Pergeseran Makna Sifat Melawan Hukum Dalam Tindak Pidana Korupsi." *Industry and Higher Education* 3, no. 1 (2021): 1689–99. <http://journal.unilak.ac.id/index.php/JIEB/article/view/3845>  
[%0Ahttps://dspace.uc.ac.id/handle/123456789/1288](https://dspace.uc.ac.id/handle/123456789/1288).

### DECLARATION OF CONFLICTING INTERESTS

The author declares that there is no conflict of interest in this article.

### FUNDING INFORMATION

None

### ACKNOWLEDGMENT

The author prays all praise and gratitude to the presence of God Almighty. Because of His blessings, mercy and grace and miracles, the author was able to complete this paper on time.

As technology advances, the  
law must adapt to protect  
rights and ensure justice