ISSN 2810-0182 (Online)
ACITYA WISESA: Journal of Multidisciplinary Research
https://journal.jfpublisher.com/index.php/jmr
Vol. 3, Issue. 2 (2024)
doi.org/10.56943/jmr.v3i2.643

Legal Liability for the Crime of Data Theft in Fake Job Postings

Sri Priyati[1], Galih Putri Sudarsono[2], Sumartini[3], Dhewangga Bayu Permana[4], Putu Angga Elano Swastika[5]*
[1]priyati@ubhara.ac.id, [2]galihputri@gmail.com, [3]sumartini@ubhara.ac.id,
[4]dhewangga@ubhara.ac.id, [5]putuanggaes@gmail.com
Faculty of Law, Universitas Bhayangkara Surabaya

*Corresponding Author: Putu Angga Elano Swastika
E-mail: putuanggaes@gmail.com

ABSTRACT

The rapid advancement of science and technology has made information technology a daily necessity, which contributes to improving the welfare of society by maintaining justice, certainty and legal expediency. In addition to the positive impacts caused, there are also negative impacts, one of which is in terms of personal data security. The focus of this research is the legal protection of job applicants as victims of criminal acts of data theft, as measured from the perspective of legal expediency. Law functions as a tool to achieve goals in society and the state, with the protection of human interests as the main focus. This research applies the empirical juridical method, which combines juridical aspects with actualities in the field on the basis of facts from research and observation. Criminal responsibility determines whether the defendant is responsible for a criminal offense that fulfills the elements of the offense. The criminal justice process follows the Criminal Procedure Code (KUHAP) and the Criminal Code (KUHP), which are the lex generalis in criminal law. The principle of Lex Specialis Derogat Legi Generali is applied to laws excluding the Criminal Code, as stipulated in Article 103 of the Criminal Code. Currently, the Electronic Information and Transaction Law is the reference; nevertheless, there are several obstacles related to the case of personal data theft. Therefore, the enactment of the Personal Data Protection Law is expected to be a solution in solving cases of personal data theft, especially those related to fake job postings.

Keywords: *Cyber Crime, Data Theft, Legal Liability, Scam*

INTRODUCTION

Interest in the use of information technology arises when users perceive the positive impact of the convenience offered by the technology (Rahman & Dewantara, 2017). In 2020, during the COVID-19 pandemic, the government declared an emergency policy ordering people to stay at home for several months. In this situation, technology became essential to carry out various activities online, including buying food, attending education, and applying for jobs. During the pandemic, people indirectly rely on technology for their daily activities, such as attending school and working remotely online.

However, the use of technology may also result in negative effects, one of which is information technology crime, such as data extortion, carding, and online fraud, which can be categorized as cybercrime. Cybercrime refers to a type of crime that occurs in cyberspace through the use of computers, mobile devices, and internet networks (Hartono & Sugiharto, 2022). Cybercriminals are usually well-versed in algorithms and programming. They can analyze, find loopholes, and break into devices with specific algorithms. After gaining control of the device, the perpetrator can easily steal data and utilize it for personal gain (Yakhmid, 2023).

Laws are established with the aim of creating harmony within society (Benuf & Hastono, 2021). The statement "Indonesia as a State of Law" and Article 1 Paragraph 3 of the 1945 Constitution emphasize that the country must act on the basis of law. Personal data is a form of privacy that shall be protected by law. Privacy is a person's right to determine which data or information about themselves may be known by others (Benuf & Hastono, 2021). Privacy is included in Human Rights (HAM), which is proven by the regulation of human rights protection in the Constitution of the Republic of Indonesia. Article 28G Paragraph 1 states that "every person shall have the right to the protection of their person, family, honor, dignity, and property under their control, and shall have the right to security and protection from threats of fear to do or not to do something which is a human right."

Cyber crime is a new type of crime in the international legal order that has not received adequate attention from states as subjects of international law (Situmeang, 2020). Cybercrime generally involves the use of computers as the main facility or target for committing crimes, either by altering or damaging the computer systems used (Situmeang, 2020). Perpetrators can also analyze how computer systems and networks work, find loopholes, and then use those loopholes to get into the system, allowing them to commit criminal acts, such as data theft, which may cause much greater losses compared to regular theft.

Therefore, according to the introduction and the problem statements that were elaborated previously, this research aims to determine how the legal provisions and perpetrators' liability for criminal acts of personal data theft in the context of fake job postings.

LITERATURE REVIEW

Cyber Crime

Cybercrime, also known as computer crime, encompasses a range of criminal activities conducted through or involving computer systems and networks. It is characterized by its occurrence in cyberspace, a virtual environment that has emerged due to the democratization of technology and globalization of networks (Fahmy, 2024; O'Regan, 2024). This form of crime includes illegal access to data, social engineering attacks, and various other malicious activities that can lead to significant political, economic, and social repercussions (Tobing et al., 2023). The rise of cybercrime necessitates a robust legal framework and international cooperation, as these offenses often transcend national borders, complicating enforcement efforts (Fahmy, 2024; Pettoello-Mantovani, 2024). Furthermore, the evolution of technology, including artificial intelligence, has introduced new challenges, prompting calls for legal adaptations to effectively address these emerging threats (Pettoello-Mantovani, 2024). As such, cybersecurity measures are critical in protecting systems and data from these evolving cyber threats (Neha, 2024).

Indonesia's cybercrime law, particularly Law No. 27 of 2022, has significant implications for the protection of personal data, addressing vulnerabilities in the digital landscape. This law aims to enhance legal protections for individuals against cyber threats, such as data breaches and unauthorized access, which are increasingly prevalent in the banking sector and e-commerce transactions (Lazuardy et al., 2024; T. I. Putra & Fibrianti, 2024; Setiawati et al., 2024). However, challenges remain, including ambiguities in accountability and the overlap with existing regulations, which can hinder effective enforcement (E. Lestari & Rasji, 2024; Rosadi et al., 2023). The law's implementation is crucial for restoring public trust in financial institutions, as it seeks to align with international standards, such as the EU GDPR, although current protections may still fall short compared to those in Europe (Rosadi et al., 2023). Overall, while the law represents a step forward, ongoing efforts are necessary to address its limitations and ensure robust personal data protection in Indonesia's evolving digital economy.

Data Theft

Data theft refers to the unauthorized acquisition of digital information, often targeting sensitive personal or organizational data, which can lead to significant privacy breaches and financial losses (Achmad et al., 2020; Al-Harrasi et al., 2023). This phenomenon poses risks not only to individual users but also to large organizations, where insider threats can exacerbate vulnerabilities (Al-Harrasi et al., 2023). Furthermore, the increasing reliance on digital platforms for everyday activities heightens the risk of personal data exposure, emphasizing the need for robust data protection strategies and public awareness to prevent negligence in data

handling (Ryazanova, 2022). Thus far, data theft remains a critical concern in the realm of information security, requiring comprehensive strategies for prevention and response (Cahyono & Hartantien, 2023).

The Indonesian government's data protection law, primarily encapsulated in Law No. 27/2022, exhibits significant gaps when compared to international standards, particularly the EU's General Data Protection Regulation (GDPR). While the Indonesian law introduces essential principles such as data subject rights and transparency, it lacks the robust enforcement mechanisms and independent oversight present in more developed frameworks like those in Singapore and Japan (Halbert et al., 2023; Rosadi et al., 2023). The absence of an independent supervisory authority further complicates effective implementation and public trust (Halbert et al., 2023). Additionally, the overlap with existing laws creates legal ambiguities that hinder comprehensive data protection efforts (E. Lestari & Rasji, 2024). Comparative analyses reveal that while Indonesia's legal framework is evolving, it still falls short of the stringent protections and accountability measures found in other jurisdictions, highlighting the need for further harmonization and regulatory refinement (Y. Lestari & Mujib, 2022; Marischa & Setianingrum, 2024).

RESEARCH METHODOLOGY

In this research, an empirical juridical approach is applied. Empirical juridical research is an approach that examines juridical problems and the actual situation in the field related to these matters (Efendi & Ibrahim, 2018). Based on the empirical approach, knowledge is based on facts obtained from research and observation. This research is focused on the legal protection of job applicants who are victims of criminal acts of data theft.

RESULT AND DISCUSSION

Legal Provisions for Criminal Offenses

In the current era of globalization, the use of information technology is progressing rapidly. This also impacts the development of the use of personal data. One of these developments is the application of e-commerce in the trade and business sector, e-education in the education sector, e-health in the health sector, e-government in government, search engines, social networks, smartphones, mobile internet, and the growth of the cloud computing sector.

However, there is also a risk of privacy violations in this era of globalization caused by the culture or behavior of people in sharing data and information. Many people voluntarily provide relatively complete personal data, such as date of birth, telephone number, address, profile picture, and many others, either intentionally or unintentionally. The open and free characteristic of the internet causes this flow of information data to take place very quickly without any control. In fact, the internet is currently used to apply for jobs without having to bother showing up at the

workplace, simply by fulfilling the necessary requirements, such as a job application letter, curriculum vitae (CV), and personal identity (Identity Card, Family Card, Taxpayer Identification Number).

As information spreads quickly and efficiently, many companies advertise job vacancies on the internet. These job vacancies are posted on social media or on websites. On the website, applicants are able to select the job vacancies they are interested in and check the requirements that must be met. Job applicants must create an account with their full identity, allowing them to easily select and search for jobs.

However, in addition to the convenience offered by technology, there are also people who take advantage of this situation to steal data for personal gain. These criminals usually use phishing methods to carry out their actions, by luring or utilizing bait that is usually in the form of fraudulent information that resembles the original.

Cases of personal data breaches frequently occur in Indonesia. According to data from the Ministry of Communication and Information, there have been 79 cases of data theft in the country since 2019 (Devansyah, 2024). From January to June 2023, 35 cases were recorded. This number exceeds the number of data breaches that occur every year. The leaked data includes personal identification numbers (NIK), provider phone numbers, and others (Hapsari & Pambayun, 2023). The modus operandi used by the perpetrators or hackers to obtain the personal data of their victims is mostly the phishing method, where the perpetrators do not directly take action, but the victims enter their own data without realizing that they have been tricked and provide or enter their personal data into the site (Vida, 2024). Victims may not realize that their data has been taken and then sold or even used to access their bank accounts.

The results of the authors' interviews with several victims who were exposed to fake job postings indicate that they experienced various problems. One of the victims claimed that some of the savings in his account were stolen; the second victim experienced an unpleasant incident, where he was often terrorized by online loan debt collectors despite the fact that he never owed money through the online loan; while the third victim said that he did not experience any problems after applying for the fake job postings.

The protection of personal data is closely related to the concept of privacy, which is the idea of maintaining the integrity and dignity of each individual. This concept of privacy is important for developed countries in relation to personal data that must be protected (Rumlus & Hartadi, 2020). Human rights, including privacy, are essential for individual freedom and dignity. Personal data is certain individual data that is stored, maintained, and maintained for its validity and confidentiality in accordance with the Regulation of the Minister of Communication and Information Technology No. 20/2016 on the Protection of Personal Data in Electronic Systems.

In the Regulation of the Minister of Communication and Information of the Republic of Indonesia No. 20/2016 on the Protection of Personal Data in Electronic Systems, electronic system owners who commit violations are only subject to administrative sanctions. Article 36 of this regulation explains that every person who obtains, manages, analyzes, stores, displays, announces, transmits, and/or disseminates personal data without rights will be subject to administrative sanctions in the form of verbal warnings, written warnings, temporary suspension of activities, and/or announcements on online sites. However, the sanctions imposed do not provide any deterrent effect.

Data Theft in Fake Job Postings in Indonesia

In Indonesia, criminal law is divided into two categories, general criminal and special criminal. For the general criminal category, the legal references are found in the Criminal Code (KUHP) and Criminal Procedure Code (KUHAP), while the special criminal refers to laws and regulations excluding the Criminal Code (Sumaryanto, 2020). Nonetheless, under the principle of Lex Specialis Derogat Legi Generali, which means that special laws override general laws, criminal laws that are apart from the general criminal law and deviate from the general criminal law, both materially and formally, must be considered (Sumaryanto, 2020). Therefore, special criminal law should be considered in terms of its substance and to whom it applies. According to Pompe, "special criminal laws have their own objectives and functions."

An example of a special criminal law is Law No. 19/2016 on the Amendment to Law No. 11/2008 on Electronic Information and Transactions, which is relevant to the case of theft of personal data related to job vacancy information. Law No. 19/2016 regulates the protection of permits, unlicensed operators, electronic system operators, and protection from illegal access. Fundamentally, these provisions cover two bases for the legitimacy of personal data processing, which are consent and positive legal norms. These two principles serve as the basis for lawful data processing. However, it is considered that the Electronic Information and Transaction Law does not clearly cover which data that should be protected in the context of personal data, as well as which types of personal data can be considered sensitive data (Rumlus & Hartadi, 2020).

In addition to Law No. 19/2016, there are other laws and regulations that aim to provide adequate protection for individuals against unauthorized use, unwanted disclosure, or misuse of personal data. It is also intended to create transparency in the use of data, give individuals the right to control their personal data, and establish responsibilities for organizations or entities that collect, manage, and process such data (BCA, 2023).

Under Law No. 27/2022 on Personal Data Protection, personal data is defined as data that can identify people directly or indirectly, either through electronic or non-electronic systems. In addition, this law also stipulates that individuals who

conduct business or e-commerce activities at home are included in the category of personal data controllers, making them legally liable for the processing of personal data carried out and must fulfill the provisions in this law.

According to Article 2 Paragraph 2 of the Personal Data Protection Law, "personal activities" or "household activities" refer to activities in the private sphere that are personal, non-commercial, and non-professional in nature. They have no liability or obligation stipulated in the Personal Data Protection Law as a controller of personal data.

Article 4 of this law distinguishes personal data into two categories:

1. Specific personal data, including health information, biometric data, genetic data, criminal records, child data, financial data, and/or any other data regulated by law.
2. General personal data, including full name, gender, nationality, religion, marital status, and/or other data used to identify an individual (Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, 2022).

Article 65 explains the prohibition on unlawfully collecting, obtaining or disclosing personal data of others. As mentioned in these articles, the Personal Data Protection Law is currently the law used to handle personal data misuse cases and has met the right criteria from the perspective of legal expediency. Law is merely a tool to achieve goals in society and the state. The purpose of law can be seen in its function as the protection of human interests. The purpose of this law itself is to provide order in people's lives by guaranteeing the right to privacy of personal data (Hisbulloh, 2021).

Criminal Liability for the Crime of Data Theft

The issue of criminal liability for criminal acts related to the granting of authority is an intriguing issue to be examined in the context of justice. This issue is intriguing because, despite the fact that the act committed is only a result of the authority granted, the person who granted the authority is not criminally liable for the act. As a result, the relationship between law and justice is important in politics. Aristotle also argued that happiness (eudaimonia), which is the ultimate goal in life, can only be achieved through the constitution of a just law (Lewokeda, 2018). Criminal liability is negatively formulated, which means that in Indonesian criminal law, as in other civil legal systems, the law formulates circumstances that may lead to the perpetrator not being held liable. In other words, as long as the perpetrator does not commit a criminal offense, they do not bear any criminal liability (Lewokeda, 2018).

Criminal liability focuses on the punishment of the perpetrator to determine whether a defendant or suspect is liable for the criminal offense that occurred. The criminal offense committed must fulfill the elements of the offense stipulated by

law. Therefore, since the conditions for punishment are similar to the offense, the elements of the offense in the prosecution must be proven in court.

An individual will be held liable if their actions are contrary to the law. Only individuals who are capable of being held liable can be convicted from the perspective of liability. The formulation of criminal liability negatively can be seen from the provisions in Articles 44, 48, 49, 50, and 51 of the Criminal Code, which establish regulations to protect the perpetrator from criminal punishment. Exclusion from criminal responsibility is intended to avoid criminal liability, which implies that in certain situations no wrongdoing is committed.

Based on the monodualistic concept (daad en dader strafrecht), the due process for determining who is responsible for a criminal offense is carried out by considering the interests of society and the individual who committed the offense. This process relies on the ability of the offender to fulfill these conditions and the conditions that can be reproached.

The concept of criminal responsibility relates to how the offender can be convicted, thus influencing the judge's decision. Each element, whether positively or negatively formulated, must be considered by the judge. Even if the Public Prosecutor does not prove this, the judge must still consider it. In this case, the judge is responsible for further investigating the defendant's testimony as to the specific circumstances of the event that rendered them guilty.

In the case of personal data theft, citizens' privacy rights are protected by the Indonesian constitution, as stated in Article 28 G Paragraph 1 of the 1945 Constitution, and repeated in Article 29 of Law No. 39/1999 on Human Rights. Indonesia has also ratified the International Covenant on Civil and Political Rights (ICCPR).

Unfortunately, the transfer of a person's personal data regardless of the owner's consent continues to occur, especially by those who store and record personal data, both by government and private institutions. In this case, specific laws, such as the Electronic Information and Transaction Law, have regulated the guarantee of personal data protection. Legal scholars, including Arthur Miller, adopt Westin's definition that describes data privacy as a person's ability to control how their personal information is disclosed. With the advancement of technology, personal data can be accessed, processed, collected and altered rapidly and affordably. Westin argues that the social obligations that are as important as the right to privacy are not absolute (Djafar et al., 2016).

Therefore, the Electronic Information and Transaction Law is used as a reference in the case of personal data protection, especially Article 32 which has been mentioned previously. The criminal liability can be found in Article 48, which states that perpetrators of personal data theft are subject to imprisonment for a maximum of 10 years and/or a maximum fine of IDR 5 billion.

In addition to the Electronic Information and Transaction Law, there is also another law that regulates data theft, which is Law No. 27/2022 on Personal Data

Protection, which is scheduled to be effective as of October 2024. This law is transnational, covering civil, administrative, and criminal aspects. In relation to the personal data theft, there is a provision stating that the perpetrators of data theft can be subject to criminal sanctions.

Perpetrator Liability in Fake Job Postings

One important step towards career success is finding a new job. In this modern era, people can easily find jobs through social media and websites. However, the rise of digital scams in Indonesia is particularly concerning, urging people to be careful when accessing the internet. Technology has provided the opportunity for criminals to take advantage of it, one of which is the phishing method. The goal of phishing is to obtain personal information voluntarily without the victim realizing it. Phishers begin their actions by using links or pictorial icons to lead users to believe that they are offering a legitimate thing. After gaining the user's trust, the perpetrator can proceed to obtain privacy data and fulfill any wishes that may disadvantage the user (I. K. O. K. Putra et al., 2023). If someone is identified as a phisher, they will be subject to penalties in accordance with the provisions in the law. Victims can report these crimes to the authorities for investigation. The disadvantages may vary, ranging from financial loss to personal data breaches. Given the wide variety of frauds, people should be more careful and wise in spending their time on the internet.

In the Electronic Information and Transaction Law, the modus operandi of phishing is regulated in Article 35 and Article 51. These two articles are interrelated and can be used as the foundation for indictments by prosecutors, Article 35 jo. Article 51 Paragraph 1. In addition, Article 28 and Article 45A are also interrelated, regulating phishing, which will be used as the basis for charges by prosecutors, Article 28 Paragraph 1 jo. Article 45A Paragraph 1.

However, there are problems in the case of personal data theft related to fake job postings, where the Electronic Information and Transaction Law does not provide a description of personal data, thus creating a legal vacuum. Therefore, the Personal Data Protection Law serves as a benchmark to address the issue of personal data theft and provides a complete explanation of personal data as well as the roles of several related agencies. In the Personal Data Protection Law, there are criminal provisions that regulate the procedural law applicable in judicial proceedings relating to the protection of personal data, as stated in Article 64 Paragraph 2. The trial can be conducted behind closed doors if necessary to protect personal data (Oktavira, 2022).

Victims are entitled to report the personal data theft to the police, in accordance with Article 12 Paragraph 1 of the Personal Data Protection Law. In addition, victims also have the right to sue and receive compensation for breaches of personal data processing in accordance with the provisions of laws and regulations.

The right to privacy requires protection of personal data by providing legal certainty for the security and order of the country (Nababan et al., 2023). The Personal Data Protection Law comes into effect in October 2024 to meet consumer demands and needs by considering personal data protection, encouraging ethically responsible innovation, and respecting human rights. According to the Personal Data Protection Law, personal data is data that directly or indirectly identifies or can identify an individual, either alone or along with other information, through electronic or non-electronic systems. Therefore, personal data protection is a comprehensive effort to protect personal data during processing, thus protecting the constitutional rights of data subjects (Puspitasari et al., 2023).

In this case, criminal liability for the perpetrator of the crime of theft of personal data in fake job postings is subject to Article 67 Paragraph 1 jo. If the perpetrator is a corporation, then Article 70 is imposed, which states that the perpetrator must be responsible for the losses caused and must compensate for the acts committed.

CONCLUSION

Legal protection against data theft related to fake job postings in Indonesia is rooted in various laws that reflect the government's constitutional responsibilities and commitment to human rights. The Criminal Code (KUHP) governs theft in general, but given the technological context of data theft, special laws take precedence, as established by the principle of lex specialis derogat legi generali. The Personal Data Protection Law categorizes personal data into specific (e.g., health and biometric data) and general data (e.g., names and genders), imposing penalties on individuals who unlawfully collect or disclose such data. This framework is critical in addressing data theft in the digital age, especially through misleading job advertisements.

Criminal liability for data theft through fake job postings is specifically outlined in the Law on Electronic Information and Transactions, with relevant articles providing criminal sanctions and fines. The recently enacted Law No. 27 of 2022 on Personal Data Protection, effective October 2024, enhances these protections by introducing harsher penalties, including imprisonment and significant fines for offenders, whether individuals or corporations. This law aims to empower victims by granting them the right to report violations and seek redress, ensuring legal certainty and promoting ethical practices in the digital realm. Ultimately, perpetrators of data theft must be held accountable for the damages caused, and the law seeks to safeguard human rights while fostering responsible innovation in technology.

REFERENCES

Achmad, A. D., Dewi, A. A., Purwanto, M. R., Nguyen, P. T., & Sujono, I. (2020). Implementation of Vigenere Cipher as Cryptographic Algorithm in Securing Text Data Transmission. *Journal of Critical Reviews*, *7*(1), 76–79. https://doi.org/10.22159/jcr.07.01.15

Al-Harrasi, A., Shaikh, A. K., & Al-Badi, A. (2023). Towards protecting organisations' data by preventing data theft by malicious insiders. *International Journal of Organizational Analysis*, *31*(3), 875–888. https://doi.org/10.1108/IJOA-01-2021-2598

BCA. (2023). *Penting Kenali UU Perlindungan Data Pribadi di Indonesia*. BCA Finance. https://bcafinance.co.id/Penting-Kenali-UU-Perlindungan-Data-Pribadi-di-Indonesia

Benuf, K., & Hastono, B. (2021). Formal Obstacles to Criminal Law Enforcement on the Crime of Personal Data Theft. *Majalah Hukum Nasional*, *51*(2), 261–279. https://doi.org/10.33331/mhn.v51i2.148

Cahyono, F. D. P., & Hartantien, S. K. (2023). Judicial Review of Criminal Offenses on Customer Data Theft of Banks Implicated in the Loss of Customer's Money. *YURIS: Journal of Court and Justice*, *2*(3), 54–68. https://doi.org/10.56943/jcj.v2i3.398

Devansyah, M. A. (2024). *Memahami Tantangan dan Solusi Terhadap Keamanan Data di Era Cloud Computing*. BINUS University. https://student-activity.binus.ac.id/himsisfo/2024/06/memahami-tantangan-dan-solusi-terhadap-keamanan-data-di-era-cloud-computing/

Djafar, W., Sumigar, B. R. F., & Setianti, B. L. (2016). *Perlindungan Data Pribadi: Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia*. Lembaga Studi dan Advokasi Masyarakat. https://books.google.co.id/books?id=PWXhvQEACAAJ

Efendi, J., & Ibrahim, J. (2018). *Metode Penelitian Hukum: Normatif dan Empiris* (Cet.2). Prenada Media Group.

Fahmy, W. (2024). The Cybercrime Acts and the Electronic Transaction in International Law. *Economics, Law and Policy*, *7*(1), p18. https://doi.org/10.22158/elp.v7n1p18

Halbert, G., Rusdiana, S., & Hutauruk, R. H. (2023). Urgensi Keberadaan Otoritas Pengawasan Independen Terhadap Harmonisasi Hukum Perlindungan Data Pribadi Di Indonesia. *Jurnal Hukum To-Ra : Hukum Untuk Mengatur Dan Melindungi Masyarakat*, *9*(3), 304–321. https://doi.org/10.55809/tora.v9i3.275

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman Cybercrime di Indonesia:

Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*, *5*(1), 1–17. https://doi.org/10.33701/jk.v5i1.3208

Hartono, D. J., & Sugiharto. (2022). The Criminal Responsibility for Pornography Video Maker Through Digital Forensics on Social Media. *YURIS: Journal of Court and Justice*, *1*(2). https://journal.jfpublisher.com/index.php/jcj/article/view/119

Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi. *Jurnal Hukum*, *37*(2), 119. https://doi.org/10.26532/jh.v37i2.16272

Lazuardy, M. S., Rachmawati, M., Marlina, T., & Umar, J. (2024). Legal Framework for Protecting Bank Customers against Personal Data Leakage in the Digital Era: A Study of Indonesian Regulations. *Indonesian Journal of Multidisciplinary Science*, *3*(10). https://doi.org/10.55324/ijoms.v3i10.907

Lestari, E., & Rasji, R. (2024). Legal Study on Personal Data Protection Based on Indonesian Legislation. *Awang Long Law Review*, *6*(2), 471–477. https://doi.org/10.56301/awl.v6i2.1206

Lestari, Y., & Mujib, M. M. (2022). Optimizing Personal Data Protection Legal Framework in Indonesia (a Comparative Law Study). *Supremasi Hukum: Jurnal Kajian Ilmu Hukum*, *11*(2), 203–234. https://doi.org/10.14421/sh.v11i2.2729

Lewokeda, K. M. D. (2018). Pertanggungjawaban Pidana Tindak Pidana terkait Pemberian Delegasi Kewenangan. *Mimbar Keadilan*, *14*(28), 183–196. https://media.neliti.com/media/publications/278234-pertanggungjawaban-pidana-tindak-pidana-12ce9bfe.pdf

Marischa, D., & Setianingrum, R. B. (2024). Transfer of Personal Data by E-Commerce Companies: A Study From The Perspective of Indonesian Personal Data Protection Laws. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, *4*(1), 48–64. https://doi.org/10.15294/ipmhi.v4i1.78267

Nababan, D. M. B., Lasmadi, S., & Erwin, E. (2023). Pertanggungjawaban Pidana Terhadap Penyalahgunaan Data Pribadi Pada Tindak Pidana Dunia Maya. *PAMPAS: Journal of Criminal Law*, *4*(2), 232–251. https://doi.org/10.22437/pampas.v4i2.26981

Neha, R. M. T. (2024). Cyber Security. *International Journal of Science and Research (IJSR)*, *13*(1), 440–444. https://doi.org/10.21275/MR231228122722

O'Regan, G. (2024). *Computer Crime* (pp. 237–252). https://doi.org/10.1007/978-3-031-52664-0_12

Oktavira, B. A. (2022). *Terjadi Pencurian Data Pribadi (Identity Theft)? Tempuh Langkah Ini*. HukumOnline.Com. https://www.hukumonline.com/klinik/a/terjadi-pencurian-data-pribadi-

tempuh-langkah-ini-lt5d904597bfa6e/

Pettoello-Mantovani, C. (2024). Cybercrimes: An Emerging Category of Offenses within the Frame of the International Criminal Court Jurisdiction. *International Journal of Law and Politics Studies*, *6*(2), 06–11. https://doi.org/10.32996/ijlps.2024.6.2.2

Puspitasari, D., Izzatusholekha, I., Haniandaresta, S. K., & Afif, D. (2023). Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Mengatasi Masalah Keamanan Data Penduduk. *JASS: Journal of Administrative and Sosial Science*, *4*(2), 195–205. https://doi.org/10.55606/jass.v4i2.403

Putra, I. K. O. K., Darmawan, I. M. A., Juliana, I. P. G., & Indriyani. (2023). Tindakan Kejahatan pada Dunia Digital dalam Bentuk Phising. *Jurnal Cyber Security Dan Forensic Digital*, *5*(2), 77–82. https://doi.org/10.14421/csecurity.2022.5.2.3797

Putra, T. I., & Fibrianti, N. (2024). 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*(1), 64–74. https://doi.org/10.32801/abc.v9i1.159

Rahman, A., & Dewantara, R. Y. (2017). Pengaruh Kemudahan Penggunaan dan Kemanfaatan Teknologi Informasi terhadap Minat Menggunakan Situs Jual Beli Online" (Studi Kasus pada Pengguna Situs Jual Beli "Z"). *Jurnal Administrasi Bisnis S1 Universitas Brawijaya*, *52*(1), 1–7.

Rosadi, S. D., Noviandika, A., Walters, R., & Aisy, F. R. (2023). Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy? *International Review of Law, Computers & Technology*, *37*(1), 78–90. https://doi.org/10.1080/13600869.2022.2114660

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik. *Jurnal HAM*, *11*(2), 285. https://doi.org/10.30641/ham.2020.11.285-299

Ryazanova, E. (2022). Responsibility for the dissemination of personal data as a way to counteract offenses in the field of information and communication technologies. *Vestnik of the St. Petersburg University of the Ministry of Internal Affairs of Russia*, *2022*(3), 118–123. https://doi.org/10.35750/2071-8284-2022-3-118-123

Setiawati, D., Permata Dewi, T., & Ayu Astutik, Z. (2024). Personal Data Protection Vulnerabilities In Cybercrime Sniffing Bank Account Break-Ins. *Yurispruden: Jurnal Fakultas Hukum Universitas Islam Malang*, *7*(2), 184–199. https://doi.org/10.33474/yur.v7i2.21184

Situmeang, S. M. T. (2020). *Cyber Law*. CV Cakra. https://elibrary.unikom.ac.id/id/eprint/4445/7/BAHAN AJAR CYBER

LAW.pdf

Sumaryanto, D. (2020). *Kapita Selekta Pidana Khusus*. Jakad Media Publishing. https://books.google.co.id/books?id=A8DZDwAAQBAJ

Tobing, M. S., Wulandari, U., Sihotang, M. S., & Raihana, R. (2023). Tinjauan Terhadap Modus-Modus Kejahatan Dalam Hukum Cyber Crime. *Jurnal Hukum Dan Sosial Politik*, *1*(2), 60–67. https://doi.org/10.59581/jhsp-widyakarya.v1i2.239

Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (2022). https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Vida. (2024). *Penyalahgunaan Data Pribadi: Contoh Kasus dan Kerugiannya*. VIDA. https://vida.id/id/blog/penyalahgunaan-data-pribadi

Yakhmid, R. Y. (2023). *Waspada Kejahatan Siber di Era Serba Daring*. LAN RI.