JURNAL HUKUM
NOVELTY
Volume 15, Issue 2, 2024, pp. 268-285

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

Data theft and the law on protection of personal data: A thematic analysis

Erwin Asmadi[1*], Adi Mansar[1], Triono Eddy[1], Mukti Fajar Nur Dewata[2], Farid Wajdi[1], Norhasliza binti Ghapa[3]

[1] *Universitas Muhammadiyah Sumatera Utara, Indonesia*
[2] *Universitas Muhammadiyah Yogyakarta, Indonesia*
[3] *Universiti Sultan Zainal Abidin, Malaysia*

*Corresponding Author: *erwinasmadi@umsu.ac.id*

Abstract

Introduction to the Problem: Data theft and leakage have severe consequences and can harm individuals, organizations, and society. Such problems also frequently occur in Indonesia massively.
Purpose/Study Objectives: This study aims to analyze the efficacy of legal measures, particularly Law Number 27 of 2022, in addressing these issues and explores challenges hindering effective enforcement.
Design/Methodology/Approach: This study employs a qualitative approach, specifically thematic analysis, to examine the legal landscape of personal data protection in Indonesia, utilizing Law Number 27 of 2022 as the primary document for analysis. The data was then transferred to Nvivo 12 Plus for coding, classification, and coding based on units of analysis, including theme identification and text search to find words, phrases, or text patterns.
Findings: The study reveals that substantial steps, including the enactment of the Personal Data Protection law, have been taken to address data theft in Indonesia. The law establishes criminal consequences, encompassing imprisonment, fines, restitution, or a combination thereof. However, despite these measures, challenges persist, including limited law enforcement capacity, insufficient awareness of data protection, constrained inter-agency cooperation, and the swift pace of technological advancements. Furthermore, issues such as limited digital evidence, sluggish legal processes, low reporting rates, ineffective penalties, and difficulties in enforcing laws in cyberspace compound the challenges faced by law enforcement in Indonesia.
Paper Type: Research Article
Keywords: Data Theft; Data Protection; Criminal Law; Adaptive Law

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

JURNAL HUKUM NOVELTY
Volume 15, Issue 2, 2024, pp. 268-285

Introduction

The rapid progress of digitalization in aspects of social, economic and government life has opened wide doors for innovation and efficiency (Baharuddin et al., 2022; Matthess & Kunkel, 2020), but unfortunately, it has also increased the risk of data theft and leakage (Wang, 2023; Zulu & Dzobo, 2023). In a social context, increasingly close connectivity through social media platforms and information-sharing applications increases the vulnerability of personal data to misuse. In the economic sector, online transactions and digital financial management allow cyber criminals to hack systems and steal financial information. Meanwhile, governments that increasingly adopt technology in providing public services and storing administrative data are also potential targets (Ibrahim et al., 2023; Mohammed et al., 2022).

The impact of advances in digitalization, especially in social, economic and government life, brings several risks of data theft and leakage that need to be considered. Connectedness via social media increases the risk of misuse of personal data, while online transactions and digital financial management open up opportunities for cybercriminals. Governments that adopt technology are also potential targets. To overcome these challenges, more robust cybersecurity measures and stricter regulations are needed to protect the interests of society, business, and government (Almaraz-Rivera et al., 2023; Andraško et al., 2021; Warikandwa, 2021).

Data theft and leakage have severe consequences and can harm individuals, organizations, and society (Abidin et al., 2019; Thaduri et al., 2019; Toma et al., 2023). In the case of Indonesia, several cases have been found indicating theft and data leakage activities. As of 2022, several significant cases of alleged personal data leaks have occurred. These data leaks include Bank Indonesia, hospital patient data leaks, job applicant data, customer data for the state electricity company (PLN), and internet service user data (Nurhadi, 2022). This often occurs in other countries (Okeke & Eiza, 2022; Solami et al., 2020).

Data theft occurs when an unauthorized person or group of people illegally access, obtain, or retrieve information or data from individuals, organizations, or computer systems without permission (Freitas & Gonçalves, 2015; Ometov et al., 2022; Viano, 2017). The goals of data theft can vary, from identity theft to financial fraud to industrial espionage (Gootman, 2016; McGee & Byington, 2015). Data thieves can steal personal information such as names, addresses, identity numbers, or combinations of passwords to commit fraud or identity theft (Gupta & Kumar, 2020; Le et al., 2019; Rodríguez & Garcia-Escartin, 2017).

An example of a case of data theft can be seen in an incident where a large company was the victim of a cyber attack that succeeded in stealing customers' personal information, such as names, addresses, identity numbers, and credit card information. This data is then used by hackers to commit financial fraud or sold on the black market (Al-Harrasi et al., 2023; Hutchings & Holt, 2017). In other cases, data theft also occurs

Article History
Submitted 20 November 2023 - Revision Required 8 February 2024 - Accepted 30 October 2024

JURNAL HUKUM
NOVELTY
Volume 15, Issue 2, 2024, pp. 268-285
P-ISSN: 1412-6834
E-ISSN: 2550-0090

in the form of industrial espionage, where hackers steal a company's trade secrets or product designs to sell to competitors, providing an unfair competitive advantage (Gill, 2022; Jones, 2008). A complete understanding of the position of this case is essential, including how the violation occurred, its impact, and the legal steps that can be taken to prosecute the perpetrator and protect the victim from further harm.

Data theft is a severe privacy and information security breach and can involve significant legal issues (Chatterjee, 2019; Talesh, 2018). Many countries currently have privacy and data protection laws governing personal data use, collection, storage, and disclosure. Violating these laws can result in lawsuits, fines, or other sanctions (Goddard, 2017; Purtova, 2018; Wachter, 2018). Perpetrators of data theft can be prosecuted and subject to prison terms and fines (Holtfreter et al., 2015; Levi, 2017).

So far, many studies on data theft have been carried out. However, very few research results have been found that simultaneously relate this topic to the development of criminal law using a thematic analysis approach, especially in Indonesia. Nevertheless, at least some trends from previous studies can be mapped. First, it is critical to comply with applicable privacy and data protection laws and adopt adequate security practices to protect personal data (Hoofnagle et al., 2019; Trepte et al., 2015). Second, data theft or similar computer crimes are regulated in various jurisdictions worldwide, including criminal law (Bechara & Schuch, 2020; Mugarura & Ssali, 2020; Wicki-Birchler, 2020).

This study seeks to fill the void of previous research by relying on thematic analysis. Accordingly, this paper can formulate two questions: (a) How can the development of criminal law in Indonesia accommodate the problem of data theft? (b) How are the challenges and obstacles in criminal law in Indonesia accommodating the problem of data theft? The answers to these two questions make it possible to find solutions to fix problems and trends in data theft cases in Indonesia and become material for the government's evaluation in developing an accommodative criminal law in the future.

Methodology

This study uses a qualitative approach with a focus on thematic analysis. The thematic analysis was chosen to maximize the analysis of data theft cases, developments, and challenges to criminal law in Indonesia. This approach was chosen to guide researchers to find official document sources for analysis. Another reason for choosing thematic analysis is that it is more flexible and accommodating in answering research questions. Relevant documents found are Law Number 27 of 2022 concerning Personal Data Protection. This representative document is used to discover the problem of data theft and the developments and challenges of criminal law in Indonesia. Overall, legal research with thematic analysis allows researchers to identify, analyze, and report critical patterns or themes in legal data, such as laws or

P-ISSN: 1412-6834
E-ISSN: 2550-0090
JURNAL HUKUM NOVELTY
Volume 15, Issue 2, 2024, pp. 268-285

court decisions. The correlation lies in the ability of thematic analysis to deeply explore complex legal issues, resulting in more structured and meaningful insights.

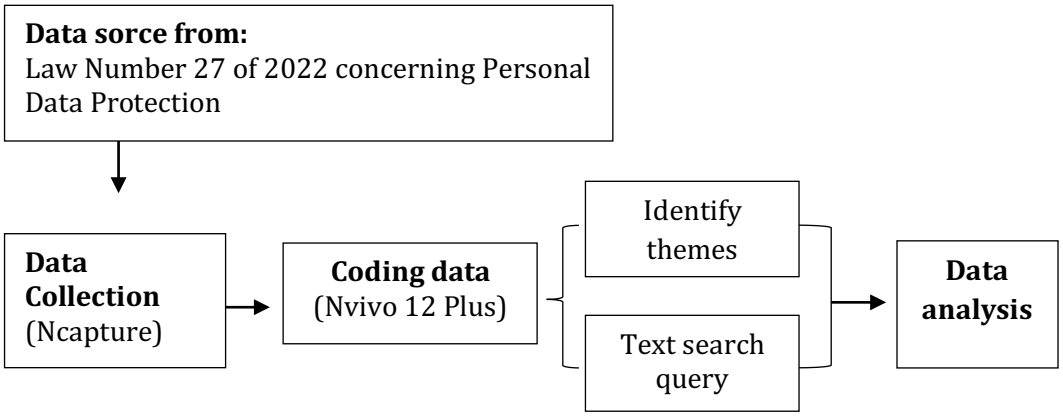

Figure 1. Data analysis process

Figure 1 shows a data analysis process, capturing data using Ncapture in Google Chrome. The data is then transferred to the Nvivo 12 Plus analysis tool for data coding. Then, classify the data and code it based on the unit of analysis, including Identifying themes and Text search queries. Identify themes are used to detect significant word phrases to identify the most frequently occurring themes. Text search queries search for specific words, phrases, or text patterns in the data (Alam, 2021; Salahudin et al., 2020). The data coding results were then followed by the visualization stage and analyzed based on trends in the data and to answer research questions.

Data validation in this research methodology is essential because it confirms the reliability of the findings resulting from a qualitative approach with thematic analysis. Using law number 27 of 2022 as a source of official documents adds to the validity of the research results, ensuring that the data analyzed is relevant and related to the issue of data theft and the development of criminal law in Indonesia. In addition, applying analysis tools such as Ncapture and Nvivo 12 Plus provides additional reliability, as both software have proven reliable in qualitative analysis, strengthening the integrity of the findings. A structured data coding process and theme identification and text search query application increased validity by providing consistent and focused analysis. The validity of the data in this research is strengthened, ensuring that the findings produced are reliable and relevant to support the research conclusions.

Results and Discussion

Law on Personal Data Protection: Accommodating Data Theft Problems in Indonesia

To accommodate the problem of data theft in Indonesia, several steps have been taken, one of which is the implementation of Law Number 27 of 2022 concerning

Article History
Submitted 20 November 2023 - Revision Required 8 February 2024 - Accepted 30 October 2024

JURNAL HUKUM
NOVELTY
Volume 15, Issue 2, 2024, pp. 268-285
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Personal Data Protection. This law has categorized several aspects as specific and general personal data.

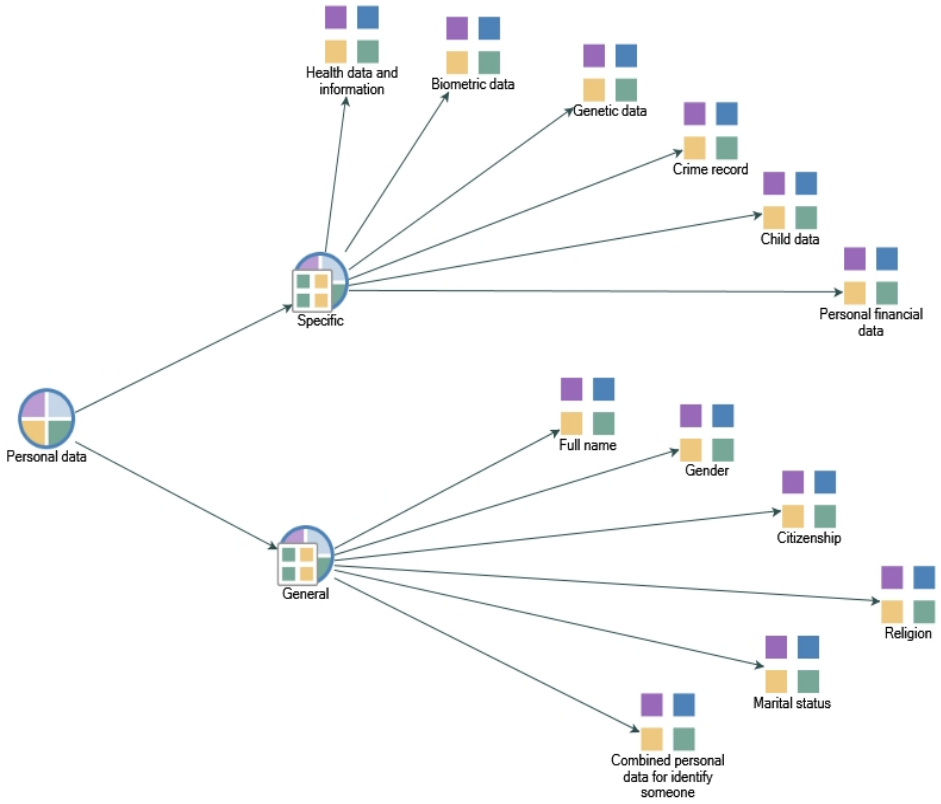

Figure 2. Personal data categories based on personal data protection laws

Figure 2 shows the categories of personal data accommodated by law in Indonesia. The data category is divided into two parts, namely specific and general personal data. Specific personal data includes health and information, biometric data, genetic data, crime records, child data, and personal financial data. Health data and information are individual records related to physical, mental, and health services. Biometric data is data related to physical, physiological, or behavioral characteristics of an individual that allows unique identification of an individual, such as facial images or dactyloscopic data. Biometric data also explains the uniqueness or characteristics of a person that must be cared for and cared for, including fingerprints, eye retinas, and DNA samples.

Genetic data are all data of any kind concerning the characteristics of an individual that are inherited or acquired during early prenatal development. In addition to these data, there are other data, namely data in the form of crime records. A crime record is a written record of someone who has committed an unlawful or unlawful act or is currently in the process of being judged for the act committed, including but not limited to police records and inclusion in the list of prevention or deterrence. Other data, namely child data, contains personal information about children, including

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

JURNAL HUKUM NOVELTY
Volume 15, Issue 2, 2024, pp. 268-285

name, date of birth, address, telephone number, and other information that can identify the child's identity. Apart from these specific personal data, other protected data is personal financial data. Personal financial data includes but is not limited to the number of bank deposits, including savings, deposits, and credit card data.

The personal data mentioned, such as health data and information, biometric data, genetic data, crime records, child data, and personal financial data, are related to legal protection. Health data includes personal medical information, such as medical history, current health conditions, medications taken, or laboratory test results. Many countries have laws governing health data protection (Abouelmehdi et al., 2018; Rashighi & Harris, 2017). Data protection laws in several countries also regulate the use and collection of biometric data, such as the California Consumer Privacy Act (CCPA) in the United States (Mulgund et al., 2021). Several countries have laws governing the use and protection of genetic data, such as the Genetic Information Nondiscrimination Act (GINA) in the United States (Feldman, 2012). Other countries also have specific child data protection laws, such as the Children's Online Privacy Protection Act (COPPA) (Zimmerle & Wall, 2019). In the United States, there are laws governing the protection of financial data, such as the Gramm-Leach-Bliley Act (GLBA) or the Payment Card Industry Data Security Standard (PCI DSS) (Nagar et al., 2021).

The differences in personal data protection lie in the type of data protected and the specific regulations governing it. For example, health data includes personal medical information that is regulated by laws such as Indonesia's Personal Data Protection Law, which is similar to regulations in many other countries that focus on protecting medical information. Biometric data, such as fingerprints or facial recognition, is regulated by laws such as the California Consumer Privacy Act (CCPA) in the United States, which provides strict guidelines on the collection and use of this data. Genetic data, which includes information about a person's genetic code, is protected by laws such as the Genetic Information Nondiscrimination Act (GINA) in the United States to prevent discrimination based on genetic information. In addition, children's data protection, as regulated in the Children's Online Privacy Protection Act (COPPA), provides exceptional protection for the data of children under a certain age. Lastly, financial data, such as bank transaction records or credit card information, is protected by laws such as the Gramm-Leach-Bliley Act (GLBA) and the Payment Card Industry Data Security Standard (PCI DSS) in the United States, which focus on security and privacy personal financial information. Each of these types of data is regulated by a different legal framework, reflecting the importance of protection according to the characteristics of the data.

Another category, namely in general personal data, includes full name, gender, nationality, religion, marital status, and personal data combined to identify a person. This general personal data is related to legal handling in several aspects, such as privacy protection, discrimination protection, and fake or fraudulent identities

Article History
Submitted 20 November 2023 - Revision Required 8 February 2024 - Accepted 30 October 2024

JURNAL HUKUM
NOVELTY
Volume 15, Issue 2, 2024, pp. 268-285
P-ISSN: 1412-6834
E-ISSN: 2550-0090

(Boerman et al., 2021; Daly, 2018; Shi, 2022). These privacy and data protection laws regulate how personal data should be handled and protected. Personal data such as religion and gender are related to protection from discrimination. The laws of many countries prohibit discrimination based on these personal characteristics in various contexts, such as employment and public service (Cobbe, 2019).

The existence of a clear criminal law has the potential to help minimize cases of data theft. Data theft refers to acts involving unauthorized collection, access, or disclosure of an individual or organization's personal data or sensitive information by unauthorized parties. Data theft seriously violates information privacy and security (Reyns & Randa, 2017; Supriyadi, 2023; van de Weijer et al., 2019). In the Indonesian context, several criminal provisions regarding data theft are described as follows.

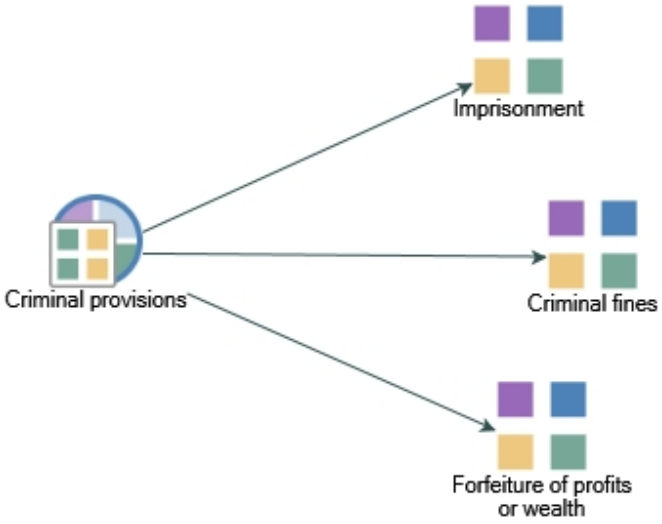

Figure 3. Criminal provisions concerning data theft

Figure 3 shows the criminal provisions regarding data theft based on Law Number 27 of 2022 concerning Personal Data Protection in Indonesia. Any person who intentionally and unlawfully obtains or collects Personal Data that does not belong to him to benefit himself or another person, which can result in the loss of the intended personal data subject, shall be punished with imprisonment and a monetary fine. In addition, additional penalties can be imposed in the form of confiscation of profits or assets obtained or proceeds from criminal acts and payment of compensation. The possible legal consequences of data theft can vary depending on jurisdiction. Some possible legal sanctions include imprisonment, fines, restitution, or a combination of these (Gottschalk & Tcherni-Buzzeo, 2017; Strom & Smith, 2017).

In cases of data theft, criminal law can provide strict sanctions to protect data and prevent similar actions in the future (Strom & Smith, 2017; van de Weijer et al., 2019). In addition to sanctions, criminal law aims to provide a deterrent effect on criminals. The deterrent effect aims to make perpetrators and others understand the severe

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

JURNAL HUKUM NOVELTY
Volume 15, Issue 2, 2024, pp. 268-285

consequences of these actions and prevent them from taking similar actions (Braga et al., 2018; Lee & McCrary, 2017). Perpetrators of data theft can be sentenced to prison as a form of criminal sanction.

The duration of a prison sentence may vary depending on the severity of the act, the harm caused, and the laws in force in the particular jurisdiction. Perpetrators of data theft can be fined as a form of sanction. The acceptable amount may also vary depending on factors such as the severity of the act, the harm caused, and the laws in force in a particular jurisdiction (Bossler, 2020; Sudarwanto & Kharisma, 2022). In some cases, perpetrators of data theft may also be required to pay restitution to victims as compensation for losses incurred due to these actions. This restitution may cover data recovery costs, additional security costs, or other financial losses the victim suffers (Eboibi & Richards, 2020; Simpson et al., 2022).

Overall, the categorization of personal data in Indonesia, as depicted in Figure 2, differentiates between specific and general personal data. Specific personal data includes health information, biometric data, genetic data, criminal records, child data, and personal financial data, each subject to legal protection. Many countries, including the United States, have enacted laws to regulate and protect specific categories of personal data, such as health, biometrics, genetics, children's information, and financial details. In addition, general personal data, which includes information such as full name, gender, nationality, religion and marital status, is also regulated by privacy and data protection laws, especially in preventing discrimination and fraudulent activities.

Figure 3 further illustrates the criminal provisions related to data theft in Indonesia, based on Law Number 27 of 2022 concerning Personal Data Protection. Legal consequences for individuals who intentionally and unlawfully collect or obtain personal data for personal gain or the benefit of others include imprisonment, monetary fines, confiscation of profits or assets, and the obligation to compensate affected parties. This level of strict sanctions is not only to punish perpetrators but also to provide a deterrent effect, deter potential perpetrators and emphasize the importance of data protection. Criminal law, therefore, plays a vital role in maintaining the security and privacy of personal data, providing punitive and preventive measures against unauthorized access or disclosure.

These findings have substantial implications regarding personal data protection policies in Indonesia. Increased awareness about strictly regulated categories of personal data, especially those of a specialized nature such as health, biometric, genetic, personal financial and children's data, provides impetus for implementing more effective security practices. Stakeholders, including individuals and organizations, can leverage this understanding to develop appropriate internal policies and data governance, ensuring that sensitive information is closely guarded.

Article History
Submitted 20 November 2023 - Revision Required 8 February 2024 - Accepted 30 October 2024

JURNAL HUKUM
NOVELTY
Volume 15, Issue 2, 2024, pp. 268-285
P-ISSN: 1412-6834
E-ISSN: 2550-0090

In a legal context, Law Number 27 of 2022 is a critical milestone confirming the Indonesian government's commitment to protecting privacy. A solid legal foundation creates the basis for addressing data breaches and providing appropriate sanctions. In addition, comparisons with data protection laws in other countries, such as the United States, indicate that Indonesia understands the importance of global linkages in building a practical framework that complies with international standards.

Apart from the legal aspects, the focus on deterring data theft through strict penalties creates a strong foundation for preventing data security breaches. Clarity of penalties and severe consequences can be a compelling incentive to deter actions that harm the privacy of individuals and organizations. It also creates a conducive atmosphere for enhancing data security culture across society and industry.

Along with this, the particular emphasis on protecting the data of children and vulnerable groups shows a deep concern for aspects of social justice. The law governing children's information creates special measures to prevent data misuse in more vulnerable groups. This creates a solid ethical footing, underscoring social and moral responsibility in protecting personal data, especially among those who need extra protection.

In facing data security and privacy challenges, governments and other stakeholders need to utilize these findings to strengthen regulations, improve law enforcement, and engage the public in efforts to protect personal data better. Public awareness of their privacy rights and the related legal consequences will form a solid basis for maintaining the integrity and security of personal data.

Challenges and Obstacles in Criminal Law in Indonesia Related to the Problem of Data Theft

There are several challenges and obstacles in criminal law related to the problem of data theft. Some must catch up to legal regulations, limited law enforcement capacity, lack of awareness and data protection, limited inter-agency collaboration, and rapid technological developments. In addition to the challenges and obstacles previously mentioned, several other obstacles include limited digital evidence, slow legal processes, and low reporting rates. The government, law enforcement agencies, and other related parties need to work together to overcome this challenge by adopting comprehensive policies, strengthening legal and technological infrastructure, increasing law enforcement capacity, and increasing public awareness and education about the importance of data protection and legal consequences related to data theft.

Law enforcement regarding data theft requires excellent technical skills and knowledge. However, not all law enforcement officials adequately understand the field of information technology and data security (Clough, 2011; Warkentin & Willison, 2009). Limited human resources, technology, and equipment can also become obstacles in investigating cases of data theft (Clough, 2011; Jarrett & Choo, 2021). Public awareness regarding the importance of protecting personal data is also

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

JURNAL HUKUM NOVELTY
Volume 15, Issue 2, 2024, pp. 268-285

considered relatively low (Hallinan et al., 2012; Mantelero, 2016). Many people need to be aware of the risks associated with data theft and are not careful about how they treat their personal information. In addition, legal protection for personal data still needs to be improved so that people can feel safe and protected.

Handling cases of data theft often involves collaboration between various agencies, such as the police, the National Cyber and Crypto Agency (BSSN), and the Ministry of Communication and Information Technology (Aulianisa & Indirwan, 2020; Mulyadi & Rahayu, 2019). Effective coordination between these agencies is challenging because of differences in priorities, authority, and understanding of legal and technical aspects. It does not stop there; the rapid development of technology also presents challenges in criminal law related to data theft. New methods of data theft are constantly emerging, such as sophisticated cyber attacks or artificial intelligence-based cyber crimes (Ozili, 2022; van de Weijer & Moneva, 2022). This requires law enforcement to adapt to new trends and techniques criminals continuously use.

To overcome these challenges and obstacles, the government, law enforcement agencies, and other related parties need to work together to overcome these challenges by adopting comprehensive policies, strengthening legal and technological infrastructure, increasing law enforcement capacity, and increasing public awareness and education about the importance of protection: data and legal consequences related to data theft. In addition, organizations and individuals need to maintain data confidentiality, implement appropriate privacy policies, and comply with relevant legal provisions to avoid violations and legal consequences that may arise.

Converting this challenge requires synergy between all stakeholders (Kesari, 2022; Ni'Mah & Syufa'at, 2021). The government must lead efforts by developing strong regulations and supporting technological infrastructure capable of dealing with the growth of cybercrime. Law enforcement agencies must be empowered with adequate resources and skills to investigate and take firm action against cybercriminals. Increasing public awareness through focused education and information campaigns will give the public a better understanding of how to protect their data and the importance of compliance with applicable laws.

In addition, the active role of organizations and individuals is vital. Organizations must implement strict data security policies, train employees on best practices in managing and protecting data, and regularly audit for compliance with privacy policies and regulations. Individuals also need to be responsible for maintaining the confidentiality of their personal information, using good cybersecurity practices, and reporting detected incidents of data theft (Njoku et al., 2023; Vajjhala & Strang, 2023). With strong collaboration between all parties, we can create an environment where personal data is managed securely and respected, reducing the risk of data theft and effectively protecting individual rights.

Article History
Submitted 20 November 2023 - Revision Required 8 February 2024 - Accepted 30 October 2024

JURNAL HUKUM
NOVELTY
Volume 15, Issue 2, 2024, pp. 268-285
P-ISSN: 1412-6834
E-ISSN: 2550-0090

On the other hand, increasing digital literacy among the public is essential in facing data security challenges. People must deeply understand how to use digital technology, the risks associated with sharing personal information online, and the actions they can take to protect themselves (Akman et al., 2023; Isabella et al., 2024; Roy, 2016). Digital education and training programs need to be expanded to include aspects of digital literacy so that individuals have sufficient knowledge to make intelligent decisions and know the consequences of their actions in the digital world.

Public awareness or vigilance also plays a crucial role in protecting data. The higher people's awareness of potential digital security risks and threats, the better they can engage in good online security practices (Al-Harrasi et al., 2023). Simple steps such as using strong passwords, avoiding clicking suspicious links, and updating software regularly can help prevent unauthorized access to personal data. Therefore, efforts to increase digital literacy and awareness must be strengthened through public information campaigns, seminars and training to help shape more responsible and safe behaviour in this digital era.

Concrete challenges and obstacles in criminal law in Indonesia regarding data theft include several essential aspects. First, legal regulations need to be updated and fully able to accommodate rapid technological developments, meaning that law enforcement often lags behind new methods of cybercrime. Second, limited law enforcement capacity, both in terms of human resources, technology, and equipment, hinders effective investigations. Third, low public awareness of the importance of protecting personal data, as well as weak collaboration between institutions, often results in suboptimal coordination in handling cases of data theft. Additionally, limited digital evidence and slow legal processes add to the complexity of resolving these cases.

Overall, increasing digital literacy and public awareness of data security is essential in facing the complex challenges in this digital era. Involving the public in risk understanding and preventive measures can form a strong foundation for personal data protection. With the government, educational institutions and the private sector playing their part, we can create a safe and trustworthy digital ecosystem. This joint effort responds to current data security risks and prepares society to face future technological developments. Therefore, continuing to prioritize digital literacy and data security awareness is an essential long-term investment in maintaining the integrity and privacy of information in an ever-evolving digital world.

Conclusion

To accommodate the problem of data theft in Indonesia, several steps have been taken, one of which is the implementation of Law Number 27 of 2022 concerning Personal Data Protection. It also encourages criminal consequences through legal sanctions, including imprisonment, fines, restitution, or a combination. Even though this has been accommodated through the law mentioned, there are still several

JURNAL HUKUM NOVELTY
P-ISSN: 1412-6834
E-ISSN: 2550-0090
Volume 15, Issue 2, 2024, pp. 268-285

challenges and obstacles, such as limited law enforcement capacity, lack of awareness and data protection, limited inter-agency collaboration, and rapid technological development are some of the factors that affect the effectiveness of law enforcement. In addition, limited digital evidence, slow legal processes, low reporting rates, limited effective penalties, and problems with enforcing the law in cyberspace are also additional factors that complicate law enforcement. Addressing this challenge requires collaborative efforts to update legal regulations, enhance law enforcement capacity, strengthen inter-agency collaboration, increase public awareness, and upgrade legal and technological infrastructure. The limitation of this research lies in the method that only considers other approaches, such as observation. Observations may provide relevant data and information to support a more profound analysis. This makes it possible for the next researcher to do so that a comprehensive analysis result is obtained to unravel the existing complexity.

Acknowledgement

Thank you to all parties involved, especially the Universitas Muhammadiyah Sumatra Utara, which has bridged this research through an accommodating discussion space.

Declarations

Author contribution : Author 1, Author 2, Author 3: initiated the research ideas, instrument construction, data collection, analysis, and draft writing; Author 4, Author 5, Author 6: review and give suggestions, literature review, data presentation and analysis, and the final draft.
Funding statement : This research was not supported by funding from other sources.
Conflict of interest : There is no conflict of interest.
Additional information : No additional information is available for this paper.

References

Abidin, M. A. Z., Nawawi, A., & Salin, A. S. A. P. (2019). Customer data security and theft: A Malaysian organization's experience. *Information and Computer Security*, *27*(1), 81–100. https://doi.org/10.1108/ICS-04-2018-0043

Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: Preserving security and privacy. *Journal of Big Data*, *5*(1), 1–18. https://doi.org/10.1186/s40537-017-0110-7

Akman, E., İdil, Ö., & Çakır, R. (2023). An investigation into the levels of digital parenting, digital literacy, and digital data security awareness among parents and teachers in early childhood education. *Participatory Educational Research*, *10*(5), 248–263. https://doi.org/10.17275/per.23.85.10.5

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

Article History
Submitted 20 November 2023 - Revision Required 8 February 2024 - Accepted 30 October 2024

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

Alam, M. K. (2021). A systematic qualitative case study: Questions, data collection, NVivo analysis and saturation. *Qualitative Research in Organizations and Management: An International Journal*, *16*(1), 1–31. https://doi.org/10.1108/QROM-09-2019-1825

Almaraz-Rivera, J. G., Cantoral-Ceballos, J. A., & Botero, J. F. (2023). Enhancing IoT network security: Unveiling the power of self-supervised learning against DDoS attacks. *Sensors*, *23*(21), 8701. https://doi.org/10.3390/s23218701

Andraško, J., Mesarčík, M., & Hamuľák, O. (2021). The regulatory intersections between artificial intelligence, data protection and cyber security: Challenges and opportunities for the EU legal framework. *AI and Society*, *36*(2), 623–636. https://doi.org/10.1007/s00146-020-01125-5

Aulianisa, S. S., & Indirwan, I. (2020). Critical review of the urgency of strenghthening the implementation of cyber security and resilience in Indonesia. *Lesrev (Lex Scientia Law Review)*, *4*(1), 33–48. https://doi.org/https: //doi.org/10.15294/lesrev.v4i1.38197

Baharuddin, T., Qodir, Z., & Loilatu, M. J. (2022). Government website performance during Covid-19 : Comparative Study Yogyakarta and South Sulawesi , Indonesia. *Journal of Governance and Public Policy*, *9*(2), 109–123. https://doi.org /10.18196/jgpp.v9i2.11474

Bechara, F. R., & Schuch, S. B. (2020). Cybersecurity and global regulatory challenges. *Journal of Financial Crime*, *28*(2), 359–374. https://doi.org/10.1108/JFC-07-2020-0149

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, *48*(7), 953–977. https://doi.org/10.1177/0093650218800915

Bossler, A. M. (2020). Cybercrime legislation in the United States. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 257–280). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-78440-3_3

Braga, A. A., Weisburd, D., & Turchan, B. (2018). Focused deterrence strategies and crime control: An updated systematic review and meta-analysis of the empirical evidence. *Criminology and Public Policy*, *17*(1), 205–250. https://doi.org/10.1111/1745-9133.12353

Chatterjee, S. (2019). Is data privacy a fundamental right in India?: An analysis and recommendations from policy and legal perspective. *International Journal of Law and Management*, *61*(1), 170–190. https://doi.org/10.1108/IJLMA-01-2018-0013

Clough, J. (2011). Data theft? cybercrime and the Increasing criminalization of access to data. *Criminal Law Forum*, *22*(1–2), 145–170. https://doi.org/10.1007/s10609-011-9133-5

Cobbe, J. (2019). Administrative law and the machines of government: Judicial review of automated public-sector decision-making. *Legal Studies*, *39*(4), 636–655. https://doi.org/10.1017/lst.2019.9

Daly, A. (2018). The introduction of data breach notification legislation in Australia: A comparative view. *Computer Law and Security Review*, *34*(3), 477–495. https://doi.org/10.1016/j.clsr.2018.01.005

Eboibi, F. E., & Richards, N. U. (2020). Electronic taxation and cybercrimes in Nigeria , Kenya and South Africa : Lessons from Europe and the United States of America.

JURNAL HUKUM NOVELTY
P-ISSN: 1412-6834
E-ISSN: 2550-0090
Volume 15, Issue 2, 2024, pp. 268-285

Commonwealth Law Bulletin, *0*(0), 1–26. https://doi.org/10.1080/03050718.2020.1726786

Feldman, E. A. (2012). The genetic information nondiscrimination act (GINA): Public policy and medical practice in the age of personalized medicine. *Journal of General Internal Medicine*, *27*(6), 743–746. https://doi.org/10.1007/s11606-012-1988-6

Freitas, P. M. F., & Gonçalves, N. (2015). Illegal access to information systems and the directive 2013/40/EU. *International Review of Law, Computers and Technology*, *29*(1), 50–62. https://doi.org/10.1080/13600869.2015.1016278

Gill, M. (2022). The handbook of security. *The Handbook of Security*, 1–1029. https://doi.org/10.1007/978-3-030-91735-7

Goddard, M. (2017). Viewpoint: The EU general data protection regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, *59*(6), 703–706. https://doi.org/10.2501/IJMR-2017-050

Gootman, S. (2016). OPM hack: The most dangerous threat to the federal government today. *Journal of Applied Security Research*, *11*(4), 517–525. https://doi.org/10.1080/19361610.2016.1211876

Gottschalk, P., & Tcherni-Buzzeo, M. (2017). Reasons for gaps in crime reporting: the case of white-collar criminals investigated by private fraud examiners in norway. *Deviant Behavior*, *38*(3), 267–281. https://doi.org/10.1080/01639625.2016.1196993

Gupta, C. M., & Kumar, D. (2020). Identity theft: A small step towards big financial crimes. *Journal of Financial Crime*, *27*(3), 897–910. https://doi.org/10.1108/JFC-01-2020-0014

Hallinan, D., Friedewald, M., & McCarthy, P. (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer Law and Security Review*, *28*(3), 263–272. https://doi.org/10.1016/j.clsr.2012.03.005

Holtfreter, K., Reisig, M. D., Pratt, T. C., & Holtfreter, R. E. (2015). Risky remote purchasing and identity theft victimization among older Internet users. *Psychology, Crime and Law*, *21*(7), 681–698. https://doi.org/10.1080/1068316X.2015.1028545

Hoofnagle, C. J., Sloot, B. van der, & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information and Communications Technology Law*, *28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: Disruption and intervention approaches. *Global Crime*, *18*(1), 11–30. https://doi.org/10.1080/17440572.2016.1197123

Ibrahim, A. H. H., Baharuddin, T., & Wance, M. (2023). Bibliometric analysis of e-government and trust : A lesson for Indonesia. *Jurnal Borneo Administrator*, *19*(3), 269–284. https://doi.org/10.24258/jba.v19i3.1303

Isabella, Alfitri, Saptawan, A., Nengyanti, & Baharuddin, T. (2024). Empowering digital citizenship in Indonesia : Navigating urgent digital literacy challenges for effective digital governance. *Journal of Governance and Public Policy*, *11*(2), 142–155. https://doi.org/https://doi.org/10.18196/jgpp.v11i2.19258

Jarrett, A., & Choo, K. R. (2021). The impact of automation and artificial intelligence on digital forensics. *WIREs Forensic Science*, *3*(6), 1–17. https://doi.org/10.1002/wfs2.1418

Jones, A. (2008). Industrial espionage in a hi-tech world. *Computer Fraud and Security*,

Article History
Submitted 20 November 2023 - Revision Required 8 February 2024 - Accepted 30 October 2024

JURNAL HUKUM
NOVELTY
Volume 15, Issue 2, 2024, pp. 268-285
P-ISSN: 1412-6834
E-ISSN: 2550-0090

2008(1), 7–13. https://doi.org/10.1016/S1361-3723(08)70010-1

Kesari, A. (2022). Do data breach notification laws reduce medical identity theft? Evidence from consumer complaints data. *Journal of Empirical Legal Studies*, *19*(4), 1222–1252. https://doi.org/10.1111/jels.12331

Le, D.-N., Kumar, R., Mishra, B. K., Khari, M., & Chetterjee, J. M. (2019). Cyber security in parallel and distributed computing: Concepts, techniques, applications and case studies. In *John Wiley & Sons*. John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119488330.ch6

Lee, D. S., & McCrary, J. (2017). The deterrence effect of prison: Dynamic theory and evidence. *Advances in Econometrics*, *38*, 73–146. https://doi.org/10.1108/S0731-905320170000038005

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: Overview and Issues: In cybercrimes, cybercriminals and their policing, in crime, law and social change. *Crime, Law and Social Change*, *67*(1), 3–20. https://doi.org/10.1007/s10611-016-9645-3

Mantelero, A. (2016). Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. *Computer Law and Security Review*, *32*(2), 238–255. https://doi.org/10.1016/j.clsr.2016.01.014

Matthess, M., & Kunkel, S. (2020). Structural change and digitalization in developing countries: Conceptually linking the two transformations. *Technology in Society*, *63*, 101428. https://doi.org/10.1016/j.techsoc.2020.101428

McGee, J. A., & Byington, J. R. (2015). Corporate identity theft: A growing risk. *Journal of Corporate Accounting & Finance*, *26*(5), 37–40. https://doi.org/https://doi.org/10.1002/jcaf.22061

Mohammed, A., Kumar, S., Mu'Azu, H. G., Kumar, R., Shah, P., Memoria, M., Rawat, A., & Gupta, A. (2022). Data security and protection: A mechanism for managing data theft and cybercrime in online platforms of educational institutions. *2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing, COM-IT-CON 2022*, 758–761. https://doi.org/10.1109/COM-IT-CON54601.2022.9850702

Mugarura, N., & Ssali, E. (2020). Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. *Journal of Money Laundering Control*, *24*(1), 10–28. https://doi.org/10.1108/JMLC-11-2019-0092

Mulgund, P., Mulgund, B. P., Sharman, R., & Singh, R. (2021). The implications of the California Consumer Privacy Act (CCPA) on healthcare organizations: Lessons learned from early compliance experiences. *Health Policy and Technology*, *10*(3), 100543. https://doi.org/10.1016/j.hlpt.2021.100543

Mulyadi, & Rahayu, D. (2019). Indonesia national cybersecurity review: Before and after establishment national cyber and crypto agency (BSSN). *2018 6th International Conference on Cyber and IT Service Management, CITSM 2018*, 1–6. https://doi.org/10.1109/CITSM.2018.8674265

Mustaufiatin Ni'Mah, A., & Syufa'at. (2021). Legalitas impor vaksin Covid-19 perspektif maqashid syariah. *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi*, *4*(1), 11–24. https://doi.org/10.24090/volksgeist.v4i1.4695

Nagar, A., Elluri, L., & Joshi, K. P. (2021). Automated compliance of mobile wallet payments for cloud services. *7th IEEE International Conference on Big Data Security on Cloud (BigDataSecurity 2021) Automated*, 38–45. https://doi.org/10.1109/BigDataSecurityHPSCIDS52275.2021.00018

JURNAL HUKUM NOVELTY
P-ISSN: 1412-6834
E-ISSN: 2550-0090
Volume 15, Issue 2, 2024, pp. 268-285

Njoku, I. S., Njoku, B. C., Chukwu, S. A. J., & Ravichandran, R. (2023). Fostering cybersecurity in institutional repositories: A case of Nigerian universities. *African Journal of Library Archives and Information Science*, *33*(1), 1–21.

Nurhadi. (2022, September 8). Inilah 7 kasus dugaan kebocoran data pribadi sepanjang 2022. *Tempo.Co*. https://nasional.tempo.co/read/1632043/inilah-7-kasus-dugaan-kebocoran-data-pribadi-sepanjang-2022

Okeke, R. I., & Eiza, M. H. (2022). The application of role-based framework in preventing internal identity theft related crimes: A qualitative case study of UK Retail Companies. *Information Systems Frontiers*, *25*, 451–472. https://doi.org/10.1007/s10796-022-10326-w

Ometov, A., Molua, O. L., Komarov, M., & Nurmi, J. (2022). A survey of security in cloud, edge, and fog computing. *Sensors*, *22*(3), 1–27. https://doi.org/10.3390/s22030927

Ozili, P. K. (2022). Central bank digital currency in Nigeria: Opportunities and risks. *Contemporary Studies in Economic and Financial Analysis*, *109*, 125–133. https://doi.org/10.1108/S1569-37592022000109A008

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40–81. https://doi.org/10.1080/17579961.2018.1452176

Rashighi, M., & Harris, J. E. (2017). Privacy in the Age of Medical Big Data. *Physiology & Behavior*, *176*(3), 139–148. https://doi.org/10.1053/j.gastro.2016.08.014.CagY

Reyns, B. W., & Randa, R. (2017). Victim reporting behaviors following identity theft victimization: Results from the national crime victimization survey. *Crime and Delinquency*, *63*(7), 814–838. https://doi.org/10.1177/0011128715620428

Rodríguez, R. J., & Garcia-Escartin, J. C. (2017). Security assessment of the Spanish contactless identity card. *IET Information Security*, *11*(6), 386–393. https://doi.org/10.1049/iet-ifs.2017.0299

Roy, J. (2016). Secrecy, security and digital literacy in an era of meta-data: Why the Canadian westminster model falls short. *Intelligence and National Security*, *31*(1), 95–117. https://doi.org/10.1080/02684527.2014.941250

Salahudin, S., Nurmandi, A., & Loilatu, M. J. (2020). How to Design qualitative research with NVivo 12 plus for local government corruption issues in Indonesia? *Jurnal Studi Pemerintahan*, *11*(3), 469–498. https://doi.org/10.18196/jgp.113124

Shi, Y. (2022). Earth observation applications and the right to privacy: Within and beyond the COVID-19 Pandemic. *Jurnal Media Hukum*, *29*(2), 107–119. https://doi.org/https://doi.org/10.18196/jmh.v29i2.14435

Simpson, S. S., Galvin, M. A., Loughran, T. A., & Cohen, M. A. (2022). Perceptions of white-collar crime seriousness: Unpacking and translating attitudes into policy preferences. *Journal of Research in Crime and Delinquency*, 1–41. https://doi.org/10.1177/00224278221092094

Solami, E. Al, Kamran, M., Alkatheiri, M. S., Rafiq, F., & Alghamdi, A. S. (2020). Fingerprinting of relational databases for stopping the data theft. *Electronics (Switzerland)*, *9*(7), 1–20. https://doi.org/10.3390/electronics9071093

Strom, K. J., & Smith, E. L. (2017). The future of crime data: The case for the national incident-based reporting system (NIBRS) as a primary data source for policy evaluation and crime analysis. *Criminology and Public Policy*, *16*(4), 1027–1048. https://doi.org/10.1111/1745-9133.12336

Sudarwanto, A. S., & Kharisma, D. B. B. (2022). Comparative study of personal data

Article History
Submitted 20 November 2023 - Revision Required 8 February 2024 - Accepted 30 October 2024

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

protection regulations in Indonesia, Hong Kong and Malaysia. *Journal of Financial Crime*, *29*(4), 1443–1457. https://doi.org/10.1108/JFC-09-2021-0193

Supriyadi, D. (2023). The Regulation of Personal and Non-Personal Data in the Context of Big Data. *Journal of Human Rights, Culture and Legal System*, *3*(1), 33–69. https://doi.org/10.53955/jhcls.v3i1.71

Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: How insurance companies Act as "compliance managers" for businesses. *Law and Social Inquiry*, *43*(2), 417–440. https://doi.org/10.1111/lsi.12303

Thaduri, A., Aljumaili, M., Kour, R., & Karim, R. (2019). Cybersecurity for eMaintenance in railway infrastructure: risks and consequences. *International Journal of System Assurance Engineering and Management*, *10*(2), 149–159. https://doi.org/10.1007/s13198-019-00778-w

Toma, T., Décary-Hétu, D., & Dupont, B. (2023). The benefits of a cyber-resilience posture on negative public reaction following data theft. *Journal of Criminology*, 1–24. https://doi.org/10.1177/26338076231161898

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? towards the "online privacy literacy scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European Data Protection Law* (pp. 333–365). Springer, Dordrecht. https://doi.org/10.1007/978-94-017-9385-8_14

Vajjhala, N. R., & Strang, K. D. (2023). Cybersecurity for Decision Makers. *Cybersecurity for Decision Makers*, 1–393. https://doi.org/10.1201/9781003319887

van de Weijer, S. G. A., Leukfeldt, R., & Bernasco, W. (2019). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*, *16*(4), 486–508. https://doi.org/10.1177/1477370818773610

van de Weijer, S. G. A., & Moneva, A. (2022). Familial concentration of crime in a digital era: Criminal behavior among family members of cyber offenders. *Computers in Human Behavior Reports*, *8*, 100249. https://doi.org/10.1016/j.chbr.2022.100249

Viano, E. C. (2017). Cybercrime: Definition, typology, and criminalization. In *Cybercrime, Organized Crime, and Societal Responses* (pp. 3–22). Springer. https://doi.org/10.1007/978-3-319-44501-4

Wachter, S. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review*, *34*(3), 436–449. https://doi.org/https://doi.org/10.1016/j.clsr.2018.02.002

Wang, Y. (2023). CNS: Research on data security technology and network data security regulations driven by digital economy. *International Journal of Cooperative Information Systems*, *32*(4), 2024. https://doi.org/10.1142/S0218843021502150009X

Warikandwa, T. V. (2021). Personal data security in South Africa's financial services market: The protection of personal information act 4 of 2013 and the european union general data protection regulation compared. *Potchefstroom Electronic Law Journal*, *24*, 17159. https://doi.org/10.17159/1727-3781/2021/v24i0a10727

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, *18*(2), 101–105. https://doi.org/10.1057/ejis.2009.12

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

JURNAL HUKUM NOVELTY
Volume 15, Issue 2, 2024, pp. 268-285

Wicki-Birchler, D. (2020). The Budapest convention and the general data protection regulation: Acting in concert to curb cybercrime? *International Cybersecurity Law Review*, *1*, 63–72. https://doi.org/10.1365/s43439-020-00012-5

Zimmerle, J. C., & Wall, A. S. (2019). What's in a Policy? evaluating the privacy policies of children's apps and websites. *Computers in the Schools*, *36*(1), 38–47. https://doi.org/10.1080/07380569.2019.1565628

Zulu, C. L., & Dzobo, O. (2023). Real-time power theft monitoring and detection system with double connected data capture system. *Electrical Engineering*, *105*(5), 3065–3083. https://doi.org/10.1007/s00202-023-01825-3

Article History
Submitted 20 November 2023 - Revision Required 8 February 2024 - Accepted 30 October 2024