SATESI Jurnal Sains Teknologi dan Sistem Informasi
journal.yp3a.org/index.php/satesi
Vol. 5 No. 1 (2025) 1 – 6 ISSN Media Elektronik: 2807–8152

The Privacy Paradox of Students' Personal Data Security in the Digital Age

Camilia Indah Novia Taufik[1], Agus Juhana[2*]
[1,2]Program Studi Pendidkan Multimedia, Kampus Daerah Cibiru, Universitas Pendidikan Indonesia, Bandung, Indonesia
Email: [1]camiliaindah7@upi.edu, [2*]agus.juhana@upi.edu

ABSTRACT

This research investigates the "privacy paradox," a phenomenon in which individuals, particularly university students, express concerns about data privacy but fail to implement effective measures to protect their personal information. The study seeks to identify key factors influencing students' awareness and behaviors concerning personal data security while proposing strategies to improve their knowledge and practices in the face of accelerating digital advancements. Employing a Systematic Literature Review using the PRISMA method, this research analyzed articles published between 2014 and 2023 to explore pertinent themes. The results indicate that students frequently disregard privacy policies and security protocols, leaving them susceptible to data breaches. Although they articulate concerns about threats from social media, university networks, and smartphones, their actions often contradict these concerns. This inconsistency arises from limited understanding of data collection processes and a perception of ineffectiveness in privacy protection efforts. The study underscores the importance of educational initiatives, such as cybersecurity training, phishing awareness programs, and the integration of advanced security technologies like blockchain and encryption. Furthermore, the enactment of Indonesia's Personal Data Protection Bill (PDP Bill) is identified as a critical step toward strengthening the legal framework for data security. Collectively, these measures aim to mitigate privacy risks and enhance students' compliance and awareness in safeguarding their personal data.

Keywords: Data Leak, Personal Data, Data Privacy, University Student.

1. Introduction

Cybersecurity is a critical issue that must be prioritized by national security and all types of businesses [1]. Previous studies indicate that protecting privacy becomes more significant when individuals use high-risk internet services [2]. Although nearly everyone is aware of cybersecurity, people's honesty and behavior are not always transparent, enabling attackers to act covertly without the victims' knowledge [3]. Both intentional and unintentional actions by computer or internet users contribute to cybersecurity breaches. For instance, users may inadvertently share or disclose passwords, access embedded links on websites, or install unverified media on their mobile devices or computers [4].

People claim to care about privacy, yet they often engage in behaviors that jeopardize their data [5]. Many users continue to rely on outdated operating systems, making it easier for attackers to access personal data illegally [6]. Although privacy settings allow users to control who can view their information, sensitive data can still be leaked [7]. Sharing limited amounts of personal data or excessive content over a short period may not immediately result in significant information exposure. However, over time, it inevitably poses substantial privacy risks [8].

The unintentional distribution of personal or sensitive data to unauthorized entities is referred to as a "data breach" or “data leaks.” However, in the context of mobile devices, researchers often describe the distribution of data to third parties without the explicit knowledge of the owner as a data leak [9]. While surveys indicate that people care about their privacy, many fail to take measures to protect it. This discrepancy between attitudes and actions is known as the "privacy paradox." Participants also feel that their efforts to safeguard privacy are futile, reflecting widespread cynicism about privacy protection [10]. Research suggests that this paradoxical behavior stems from a lack of knowledge. Although individuals are concerned about privacy, their limited understanding of how data is collected and used hinders them from taking appropriate actions. Many respondents use privacy protection tools, but often not out of personal concern for their privacy [10]. The privacy paradox suggests that concerns about online privacy are insufficient to fully explain behavior on social networking sites (SNS) [11].

Diterima Redaksi: 18-11-2024 | Selesai Revisi: 16-12-2024 | Diterbitkan Online: 20-04-2025

Previous studies indicate that internet users have limited or no knowledge about the data being tracked, collected, and stored by companies and digital technologies [12]. Some students admit to rarely reading privacy policies before downloading applications, reflecting a low level of awareness regarding personal data security [13]. Participants expressed concerns about various threats, ranging from social media and university networks to smartphones and digital wallets [14]. Users tend to feel their privacy has been violated when they believe they lack control over their personal information on social media platforms, thereby heightening their privacy concerns [15]. However, respondents demonstrated strong motivation to protect their devices and data. Applications with clear and transparent privacy policies were generally more trusted by users [6], [16]. When informed about the risks of data breaches, respondents were more likely to reduce their intention to use online platforms that could endanger their personal data [17]. Therefore, implementing effective privacy protection mechanisms is essential to address the issue of data breaches [18].

Although many claim to care about privacy and data security, research shows that their behavior often does not align with these attitudes, a phenomenon known as the "privacy paradox." Students, like many other users, often lack a full understanding of the risks and mechanisms behind the collection and use of personal data by third parties. This lack of awareness makes them more vulnerable to data breaches, which can occur either intentionally or unintentionally.

Among university students, the low level of awareness regarding data security is evident in their habit of rarely reading privacy policies before downloading applications, despite their concerns about security risks from social media and campus networks. Many users recognize the importance of privacy but fail to take concrete steps to protect it.

Furthermore, the objective of this study is to identify the variables that influence students' awareness and actions regarding the management of personal data. This research aims to offer solutions for students to be more cautious in safeguarding their personal data amidst the rapid and complex advancements in digital technology. Therefore, conducting this study is essential to enhance students' awareness of the importance of protecting personal data and to develop effective solutions to address the issues arising from data breaches that have already occurred.

2. Methods

2.1. Data Collection

The method used is a Systematic Literature Review, employing the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) method [19]. Article searches were conducted on September 22, 2024, using the Publish or Perish application with the Google Scholar database.

2.2. Research Stages

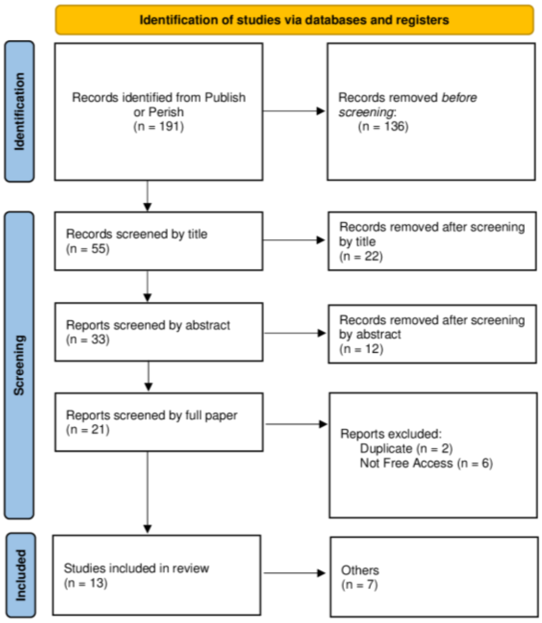
Identification of studies via databases and registers
Identification
Records identified from Publish or Perish (n = 191)
Records removed *before screening*: (n = 136)
Screening
Records screened by title (n = 55)
Records removed after screening by title (n = 22)
Reports screened by abstract (n = 33)
Records removed after screening by abstract (n = 12)
Reports screened by full paper (n = 21)
Reports excluded:
Duplicate (n = 2)
Not Free Access (n = 6)
Included
Studies included in review (n = 13)
Others (n = 7)

Figure 1. PRISMA Diagram

Based on figure 1, the search was conducted using the keywords "college students" OR "university students" AND "personal data" AND "data privacy" AND "data leakage." The search was limited to articles published between 2014 and 2023, with a maximum of 1,000 results, yielding 191 articles. After conducting the search using the Publish or Perish application, the results were transferred to Mendeley Desktop. In Mendeley Desktop, the article data was entered and then "Update Details" was applied to automatically complete any missing information in the article details.

After importing the data from Mendeley Desktop into Excel, several sorting steps were performed, starting with sorting by publisher, which resulted in 55 articles. This sorting was based on the publisher or the journal publisher indexed by SCOPUS. Next, sorting by title was performed, leaving 33 articles. This sorting was based on article titles that were relevant or related to the keywords of this study. Subsequently, sorting by abstract reduced the selection to 21 articles, with one article not available in the online database. At this stage, abstracts were read, and articles were selected based on their relevance to the study. Finally, sorting by full paper left 13 articles, with 2 duplicates and 6 articles that could not be accessed for free. In this final step, articles were reviewed in their entirety, and only those that directly addressed or were related to the research were retained.

3. Results and Discussion

Society claims to care about privacy, yet often engages in behaviors that jeopardize their data. The discrepancy between concern and action is known as the Privacy Paradox. Despite this, users rarely take advantage of the available settings to protect their privacy [5]. While surveys indicate that people care about their privacy, many fail to take measures to protect it. Participants also feel that their privacy protection efforts are futile, reflecting widespread cynicism about privacy [10]. Research shows that this paradoxical behavior is due to a lack of knowledge. Although individuals care about privacy, their limited understanding of how data is collected and used makes it difficult for them to take appropriate action. This may explain why, so far, no significant correlation has been established between behavior and privacy concerns [11]. Many respondents use privacy protection tools, but often not out of personal concern for their privacy [10]. In fact, some students admitted that they rarely read privacy policies before downloading or accessing an app, indicating a low level of awareness regarding personal data security [13]. The phenomenon of the Privacy Paradox illustrates a mismatch between individuals' concerns about online privacy and their high levels of personal information sharing. This indicates that while many internet users acknowledge the importance of privacy, they continue to share substantial amounts of personal information online [20].

Social media applications collect, display, and share personal information to enable user interaction. Users entrust their personal data, such as health information, location, or device IDs, to these applications. However, they often rely on unclear or misleading documentation to understand how their data is used and managed [21]. Despite many users expressing concerns, the number of mobile app downloads worldwide continues to rise. Users continue to download apps with little hesitation, even when the apps request excessive permissions. They weigh the risks and benefits, and despite concerns, these are often outweighed by the desire to use the app, time constraints, or the satisfaction promised by the app [22]. A lack of understanding of privacy risks can lead to apathy toward privacy issues. Individuals who do not comprehend the importance of privacy are more likely to share information without considering the potential consequences [20]. Additionally, users feel they can manage their privacy settings, yet they also perceive these efforts as futile [13].

Educational programs can raise awareness about smartphone security, as users are often unaware of the dangers associated with their devices [23]. User behavior is directly correlated with mobile phone security. Compared to other computing systems, mobile devices are considered more vulnerable to breaches due to their small size and portability [24]. Additionally, users tend to prefer faster phones over more secure ones, which can pose risks in certain situations, such as when individuals use their smartphones for online transactions [25].

Some people believe that devices like smart speakers do not capture sensitive data that is considered insignificant. However, users of these smart speakers are often unaware of the potential privacy breaches that - could occur through these devices [26]. Research indicates that respondents tend to increase their efforts to protect themselves and become more cautious about using online platforms indiscriminately [17]. Many people still use older operating systems, which make them more vulnerable to attackers. However, some individuals show a strong motivation to protect their devices and data [6]. Similarly, students express concern and awareness about various threats, ranging from social media to university or campus networks, as well as from their smartphones [14].

Raising user awareness about the importance of protecting personal data can reduce the risk of privacy breaches. It is essential to implement an effective protection model that includes user consent, clear objectives, and transparency in data processing [27]. There is a need for digital security education, starting with students. This includes understanding the risks associated with the use of applications and social media, as well as how to protect their personal data [28]. Additionally, it is important to identify vulnerabilities and provide training on information security, including how to recognize phishing attempts. There are also game-based applications designed to educate users about phishing [29].

The integrity and confidentiality of data are maintained through network protection and encryption. Users are often unaware of the significant risks involved when installing applications or updating files. Before registering and accessing data, users should ensure that the website is secure by checking key security features [30]. Although users are informed about app permissions, these permissions are often accepted without much consideration. Knowing the apps that are downloaded and the permissions they request is an important step in maintaining security [31]. There is also the possibility that information may be shared with unauthorized parties [32]. Privacy settings on social networking sites (SNS) serve as a means to regulate the boundaries of privacy between passive and active activities [33].

To mitigate the impact of data breaches, especially those that are unintentional, unauthorized recipients will be prevented from opening or accessing sensitive data [34]. By providing clear information about privacy breaches, users will gain a better understanding of the risks associated with privacy loss [35]. A thorough understanding of data issues is crucial for technical research, as it forms the foundation for data processing and protection by systems. The distinction between personal information and sensitive personal information must be acknowledged by all parties, as data protection must be tailored to the level of sensitivity. The more sensitive the data, the greater the potential harm if it is lost, leaked, or misused [36].

Online Social Networks (OSNs) play a crucial role in modern life for maintaining human relationships.

DOI: 10.54259/satesi.v5i1.3417

However, the widespread use of OSNs leads to privacy issues due to the extensive sharing of personal data online. Although privacy settings allow users to control who can view their information, sensitive data can still be leaked [7]. To protect data security and privacy in urban computing, secure data processing systems utilize blockchain and differential privacy [37]. Blockchain-based systems can significantly reduce the risks of breaches, tampering, and data corruption, safeguarding data security and privacy to a level that cannot be achieved by other existing systems [38].

It is recommended to use network analysis to enhance cybersecurity awareness. This initiative can begin with students, who can collaborate with schools or universities. Protecting personal data in education through information technology is crucial. Universities can provide training to help students recognize and mitigate cybersecurity threats [32], [39]. Additionally, the Indonesian government has drafted the Personal Data Protection Bill (PDP Bill). Despite some limitations, the enactment of this bill will be an important step for Indonesia to align its data protection laws with international standards [40].

Although students, or even society at large, may express concern about data privacy, they often act without considering security risks, such as neglecting device security regulations or failing to read privacy policies. This is known as the "privacy paradox," where knowledge of data privacy is often not followed by appropriate actions. Some students are concerned about privacy threats from social media and university networks but are not highly motivated to protect themselves. They struggle to take the necessary steps due to a lack of understanding of how personal data is collected and managed. As a result, their behavior tends to be vulnerable to the risks of data breaches.

It is crucial to provide lessons focused on information security, identifying potentially harmful digital applications, and safeguarding privacy on social media. Universities or campuses can offer training on how to identify threats such as phishing and use security software. Additional protection can also be implemented by adopting contemporary security technologies, such as blockchain systems and data encryption systems. Furthermore, laws such as the Personal Data Protection Bill (PDP Bill) will provide a strong legal foundation for securing personal data, thereby enhancing students' awareness and compliance with privacy protection measures.

4. Conclusion

This study shows that although people talk about privacy, many do nothing to protect their personal data, creating what is known as the Privacy Paradox. People are unaware of how data collection works, which makes it difficult for them to take the appropriate actions, despite their concerns. Users of social media applications and other technologies often neglect their privacy settings, thereby increasing the risk of unintended data breaches.

Furthermore, the challenge in protecting privacy stems from user behavior, which often involves granting permissions to applications without considering the associated risks, as well as a lack of understanding regarding data vulnerabilities. While some users are highly motivated and aware of the need to protect their devices and data, others feel that such efforts are futile. Therefore, it is crucial to educate users on the importance of safeguarding their personal data through training. Educational programs on data security, particularly on how to recognize threats such as phishing, are essential for raising awareness. This includes increasing cybersecurity awareness through network analysis, implementing robust protection models, and fostering collaboration between educational institutions and government agencies.

With the Personal Data Protection Bill (PDP Bill) currently under development, Indonesia has the opportunity to align its data protection laws with international standards, as personal data protection must be adapted to the increasing sensitivity of data in the digital world. It is hoped that such measures will help enhance information security in the digital era and reduce the likelihood of data breaches.

As a follow-up to this research, it is recommended to conduct further studies on educational programs or training specifically focused on personal data security, particularly for students. Additionally, further research on blockchain and encryption technologies, and their application to students in protecting data in the digital era, should be explored. Further investigation into the impact of social media on data privacy awareness is also suggested.

SUMBER RUJUKAN
Referensi

[1] A. Mishra, Y. I. Alzoubi, A. Q. Gill, and M. J. Anwar, "Cybersecurity Enterprises Policies: A Comparative Study," 2022, *mdpi.com*. doi: 10.3390/s22020538.

[2] W. Yu and F. Shen, "The relationship between online political participation and privacy protection: evidence from 10 Asian societies of different levels of cybersecurity," *Behaviour and Information Technology*, vol. 41, no. 13, pp. 2819–2834, 2022, doi: 10.1080/0144929X.2021.1953597.

[3] N. Kshetri, Vasudha, and D. Hoxha, "KnowCC: Knowledge, Awareness of Computer & Cyber Ethics between CS/Non-CS University Students," *Proceedings - 4th IEEE 2023 International Conference on Computing, Communication, and Intelligent Systems, ICCCIS 2023*, pp. 298–304, 2023, doi: 10.1109/ICCCIS60361.2023.10425385.

[4] R. Rohan, S. Funilkul, D. Pal, and W. Chutimaskul, "Understanding of Human Factors in Cybersecurity: A Systematic Literature Review," *2021 International Conference on Computational Performance Evaluation, ComPE 2021*, pp. 133–140, 2021, doi: 10.1109/ComPE53109.2021.9752358.

[5] M. Williams, J. R. C. Nurse, and S. Creese, “Smartwatch games: Encouraging privacy-protective behaviour in a longitudinal study,” *Comput Human Behav*, vol. 99, no. April, pp. 38–54, 2019, doi: 10.1016/j.chb.2019.04.026.

[6] P. Shah and A. Agarwal, “Cybersecurity behaviour of smartphone users in India: an empirical analysis,” *Information and Computer Security*, vol. 28, no. 2, pp. 293–318, 2020, doi: 10.1108/ICS-04-2019-0041.

[7] H. Robert, “Institutional Knowledge at Singapore Management University ScienceDirect Privacy leakage analysis in online social Privacy leakage analysis in online social networks networks,” pp. 239–254, 2015.

[8] X. Li, C. Zhao, Y. Hu, H. Xie, Y. Wang, and J. Zhao, “Precursor of privacy leakage detection for individual user,” *Comput Secur*, vol. 142, no. April, 2024, doi: 10.1016/j.cose.2024.103879.

[9] I. Shklovski and E. Grönvall, “CreepyLeaks: Participatory Speculation Through Demos,” *ACM International Conference Proceeding Series*, 2020, doi: 10.1145/3419249.3420168.

[10] Z. Wang and Z. Chen, “Analysing the Causes and Implications of the Privacy Paradox: Consumer Surveillance and Online Data Collection,” *Bull Sci Technol Soc*, vol. 43, no. 3–4, pp. 86–93, 2023, doi: 10.1177/02704676231220842.

[11] T. Dienlin and S. Trepte, “Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors,” *Eur J Soc Psychol*, vol. 45, no. 3, pp. 285–297, 2015, doi: 10.1002/ejsp.2049.

[12] C. Prince, N. Omrani, and F. Schiavone, “Online privacy literacy and users’ information privacy empowerment: the case of GDPR in Europe,” *Information Technology and People*, vol. 37, no. 8, pp. 1–24, 2023, doi: 10.1108/ITP-05-2023-0467.

[13] S. Havelka, “Typologies of Mobile Privacy Behavior and Attitude: A Case Study Comparing German and American Library and Information Science Students,” *Serials Librarian*, vol. 81, no. 1, pp. 42–58, 2021, doi: 10.1080/0361526X.2021.1875961.

[14] A. Farooq, S. R. U. Kakakhel, S. Virtanen, and J. Isoaho, “A taxonomy of perceived information security and privacy threats among IT security students,” *2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*, pp. 280–286, 2016, doi: 10.1109/ICITST.2015.7412106.

[15] K. C. Chung, C. H. Chen, H. H. Tsai, and Y. H. Chuang, “Social media privacy management strategies: A SEM analysis of user privacy behaviors,” *Comput Commun*, vol. 174, no. April, pp. 122–130, 2021, doi: 10.1016/j.comcom.2021.04.012.

[16] H. I. Maseeh *et al.*, “Exploring the privacy concerns of smartphone app users: a qualitative approach,” *Marketing Intelligence and Planning*, vol. 41, no. 7, pp. 945–969, 2023, doi: 10.1108/MIP-11-2022-0515.

[17] M. Feng, B. Hu, Y. Tian, and H. Wang, “Data leaking scandal, risks, and financial consumption behaviors in online tourism platforms: The role of trust on college students and teachers,” 2022, *frontiersin.org*. doi: 10.3389/fpsyg.2022.968271.

[18] J. Wang, G. Liu, and G. Zhao, “Two-attribute privacy protection method of MCS based on blockchain smart contract,” *Comput Commun*, vol. 193, no. June, pp. 126–135, 2022, doi: 10.1016/j.comcom.2022.06.045.

[19] D. Moher *et al.*, “Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement,” *PLoS Med*, vol. 6, no. 7, 2009, doi: 10.1371/journal.pmed.1000097.

[20] T. Dienlin, P. K. Masur, and S. Trepte, “A longitudinal analysis of the privacy paradox,” *New Media Soc*, vol. 25, no. 5, pp. 1043–1064, 2023, doi: 10.1177/14614448211016316.

[21] D. E. Krych and P. McDaniel, “Exposing Android social applications: linking data leakage to privacy policies,” *Journal of Cyber Security Technology*, vol. 5, no. 3–4, pp. 139–190, 2021, doi: 10.1080/23742917.2019.1630093.

[22] S. Barth, M. D. T. de Jong, M. Junger, P. H. Hartel, and J. C. Roppelt, “Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources,” *Telematics and Informatics*, vol. 41, no. November 2017, pp. 55–69, 2019, doi: 10.1016/j.tele.2019.03.003.

[23] A. Das and H. U. Khan, “Security behaviors of smartphone users,” *Information and Computer Security*, vol. 24, no. 1, pp. 116–134, 2016, doi: 10.1108/ICS-04-2015-0018.

[24] S. Mujeye, “An analysis of differences in behaviors and practices of security-conscious users and regular users on mobile devices,” *Information and Computer Security*, vol. 31, no. 5, pp. 624–634, 2023, doi: 10.1108/ICS-05-2023-0086.

[25] P. Fehér-Polgár and Z. Németh, “Safety consciousness of the mobile phone users,” *SACI 2016 - 11th IEEE International Symposium on Applied Computational Intelligence and Informatics, Proceedings*, pp. 345–348, 2016, doi: 10.1109/SACI.2016.7507399.

[26] A. Jayatilleke, S. Thelijjagoda, and P. Pathirana, “Security Awareness among Smart Speaker Users,” *2019 National Information Technology Conference, NITC 2019*, pp. 8–10, 2019, doi: 10.1109/NITC48475.2019.9114497.

[27] J. Liu and S. Zhou, “Application Research of Data Mining Technology in Personal Privacy Protection and Material Data Analysis,” *Integrated Ferroelectrics*, vol. 216, no. 1, pp. 29–42, 2021, doi: 10.1080/10584587.2021.1911255.

[28] A. H. M. Bradley and A. L. Howard, “Stress and Mood Associations With Smartphone Use in University Students: A 12-Week Longitudinal Study,” *Clinical Psychological Science*, vol. 11, no. 5, pp. 921–941, 2023, doi: 10.1177/21677026221116889.

[29] J. Rastenis, S. Ramanauskaite, J. Janulevicius, and A. Cenys, “Credulity to Phishing Attacks: A Real-World Study of Personnel with Higher Education,” *2019 Open Conference of Electrical, Electronic and Information Sciences, eStream 2019 - Proceedings*, 2019, doi: 10.1109/eStream.2019.8732169.

[30] G. Alsadoon, “Comparisons and appropriate solutions to prevent data threats of cloud computing, applied in green environment,” *2019 8th International Conference on Modeling Simulation and Applied Optimization, ICMSAO 2019*, 2019, doi: 10.1109/ICMSAO.2019.8880344.

[31] J. Walls and K. K. R. Choo, *A Study of the Effectiveness Abs Reliability of Android Free Anti-Mobile Malware Apps*. Elsevier Inc., 2017. doi: 10.1016/B978-0-12-804629-6.00008-0.

[32] R. Isus, K. Kolesnikova, I. Khlevna, T. Oleksandr, and K. Liubov, “Development of a model of personal data protection in the context of digitalization of the

educational sphere using information technology tools," *Procedia Comput Sci*, vol. 231, no. 2023, pp. 347–352, 2024, doi: 10.1016/j.procs.2023.12.215.

[33] P. Schmidt *et al.*, "Twitter Users' Privacy Behavior: A Reasoned Action Approach," *Social Media and Society*, vol. 8, no. 3, 2022, doi: 10.1177/20563051221126085.

[34] M. Guri, R. Puzis, K. K. R. Choo, S. Rubinshtein, G. Kedma, and Y. Elovici, "Using malware for the greater good: Mitigating data leakage," *Journal of Network and Computer Applications*, vol. 145, no. September 2018, p. 102405, 2019, doi: 10.1016/j.jnca.2019.07.006.

[35] Y. Wang, Y. Chen, F. Ye, H. Liu, and J. Yang, "Implications of smartphone user privacy leakage from the advertiser's perspective," *Pervasive Mob Comput*, vol. 53, pp. 13–32, 2019, doi: 10.1016/j.pmcj.2018.12.006.

[36] R. Belen Saglam, J. R. C. Nurse, and D. Hodges, "Personal information: Perceptions, types and evolution," *Journal of Information Security and Applications*, vol. 66, no. March, p. 103163, 2022, doi: 10.1016/j.jisa.2022.103163.

[37] G. Heo and I. Doh, "Blockchain and differential privacy-based data processing system for data security and privacy in urban computing," *Comput Commun*, vol. 222, no. April, pp. 161–176, 2024, doi: 10.1016/j.comcom.2024.04.027.

[38] S. Gabrielli, S. Rizzi, O. Mayora, S. More, J. C. P. Baun, and W. Vandevelde, "Multidimensional Study on Users' Evaluation of the KRAKEN Personal Data Sharing Platform," 2022, *mdpi.com*. doi: 10.3390/app12073270.

[39] M. T. B. Hoang, D. Dang-Pham, A. P. Hoang, B. Le Gia, and M. Nkhoma, "Network Analytics for Improving Students' Cybersecurity Awareness in Online Learning Systems," *Proceedings - 2020 RIVF International Conference on Computing and Communication Technologies, RIVF 2020*, 2020, doi: 10.1109/RIVF48685.2020.9140781.

[40] S. D. Rosadi, A. Noviandika, R. Walters, and F. R. Aisy, "Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy?," *International Review of Law, Computers and Technology*, vol. 37, no. 1, pp. 78–90, 2023, doi: 10.1080/13600869.2022.2114660.

DOI: 10.54259/satesi.v5i1.3417