JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v5i2

Personal Data Protection for Online Job Seekers in the Mode of Freelance Job Vacancy Fraud

Ela Suryani[1], Rasji[2].
[1]Faculty of Law, Tarumanagara University, Indonesia, ela.205210207@stu.untar.ac.id.
[2]Faculty of Law, Tarumanagara University, Indonesia, rasji@fh.untar.ac.id.

Corresponding Author: ela.205210207@stu.untar.ac.id[1]

Abstract: Digitalization has brought convenience in job search, but it also raises the risk of misuse of personal data, especially through the fraudulent mode of freelance job vacancies. This research aims to analyze the legal responsibility of digital platforms in protecting users' personal data as well as the implementation of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) in handling cybercrime cases. The research method used is qualitative descriptive, with a literature study approach to relevant regulations and cases that occur. The results of the study show that digital platforms have an obligation to ensure the security of user data, including by implementing a verification system and preventing data leaks. The PDP Law provides a strong legal basis in protecting the rights of personal data owners, but its implementation still requires increased public awareness and stricter supervision.

Keyword: Personal Data, Job Vacancy Fraud, Personal Data Protection Laws.

INTRODUCTION

The development of digital technology has brought significant changes to job-seeking mechanisms, with online platforms now becoming the primary solution relied upon by job seekers, particularly those interested in flexible jobs such as freelancing. These digital platforms provide various conveniences, including faster access to information and significant time efficiency compared to conventional methods (Matheus, 2021). However, this transformation is not without challenges, one of which is the threat to personal data protection. In some cases, job seekers' data uploaded through digital platforms can be misused by irresponsible parties, leading to losses in terms of privacy and potential data exploitation.

Fraud schemes in job vacancy scams often involve manipulative efforts to obtain personal data from prospective victims, such as identity information, residential addresses, and financial details. This data is then unlawfully used to harm the victims, including identity theft, misuse of financial information, or other illegal activities (Fikri & Rusdiana, 2023). This phenomenon highlights significant weaknesses in the management and protection systems for data on digital platforms, which should ensure user information security. It also underscores the need to

strengthen regulations and data protection mechanisms, including implementing stricter cybersecurity standards to prevent similar violations in the future.

Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) was designed as a strong legal foundation to safeguard individuals' rights over their personal data, particularly from the risks of theft or misuse by irresponsible parties (Djafar & Santoso, 2019). The regulation explicitly outlines how personal data must be managed, from the collection and storage process to its utilization, placing explicit consent from the data owner as a primary requirement. Additionally, the PDP Law emphasizes the importance of transparency in data management, ensuring that data owners clearly understand the purposes and methods of processing their data. Furthermore, the law obligates entities processing data to take adequate preventive measures to avoid data breaches, ensuring that the protection of personal data is not solely an individual's responsibility but also a legal obligation for businesses and relevant institutions.

One of the main challenges in implementing the PDP Law lies in its lack of effective enforcement, particularly in the digital platform domain. This is evident in the handling of online job fraud cases, which are becoming increasingly rampant (Hisbulloh, 2021). A significant obstacle is the low level of public awareness about the importance of protecting personal data, leading many individuals to overlook the risks involved. Moreover, supervision of digital platform providers remains insufficient, leaving gaps for perpetrators to exploit system vulnerabilities. These conditions highlight the urgent need to improve digital literacy among the public while strengthening regulations and oversight of platform operators to ensure the security of job seekers' personal data.

Previous research has tended to focus on personal data protection within the context of general regulations or data security in the information technology sector, leaving limited discussion on the legal responsibilities of digital platforms in specific cases such as freelance job fraud (Palinggi & Limbongan, 2020). This study aims to fill that gap by providing an in-depth analysis of the role of digital platforms as data controllers and the implementation of the PDP Law in addressing increasingly complex fraud schemes. The contribution of this research lies in exploring the legal responsibilities that can be imposed on digital platforms as a form of protection for job seekers. This study also offers strategic recommendations to strengthen data verification mechanisms and public education on the importance of safeguarding personal information. The article is expected to provide new insights and concrete solutions for improving personal data security in the digital era and serve as an essential reference for developing data protection policies in Indonesia.

METHOD

This study uses a descriptive qualitative approach to analyze the legal responsibility of digital platforms in protecting users' personal data and the implementation of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) in handling cases of freelance job vacancy fraud. This approach was chosen because of its relevance in exploring social and legal phenomena in depth, as well as to explore complex information about the management and protection of personal data in the digital era (Sinaga & Putri, 2020).

RESULTS AND DISCUSSION

In the increasingly developing digital era, personal data protection is one of the crucial issues, especially with the increasing prevalence of fraud through online job vacancies. This mode often takes advantage of negligence in the management of personal data, which is often overlooked by many digital platforms. Therefore, it is important to review the legal responsibility of digital platforms in protecting the personal data of their users, as well as the application of the PDP Law in overcoming cybercrime cases. In this discussion, it will be

reviewed how the legal obligations of digital platforms as data controllers and the role of the PDP Law in tackling crime cyber involving the misuse of personal data.

Legal Liability of Digital Platforms

Digital platforms function as controllers of users' personal data in cyberspace. The legal responsibility of digital platforms is very important to maintain user trust and ensure the protection of personal data in accordance with applicable legal provisions. The PDP Law clearly regulates the obligations of data controllers, including digital platforms, in managing personal data in a transparent, secure, and in accordance with the basic principles of data protection (Hisbulloh, 2021). As data controllers, digital platforms are required to obtain consent from users before collecting and processing their personal data, as stipulated in Article 27 of the PDP Law which requires explicit consent from the data owner. Transparency is an important aspect of this obligation. Digital platforms are obliged to provide clear information on how users' personal data is collected, used, and processed. Every digital platform is also required to provide a privacy policy that users can easily understand, which explains how user data is collected, stored, and shared. The lack of coordination between agencies is also an obstacle in the implementation of the PDP Law in cybercrime cases. In many cases, authorized agencies such as Ministry of Communication and Information Technology or the Personal Data Protection Authority do not have an effective mechanism to overcome and crack down on violations related to personal data protection (Sinaga & Putri, 2020).

Article 28 of the PDP Law requires data controllers to notify data owners in the event of a personal data leak within a certain time after the leak. This prompt notification allows the data owner to take the necessary protection measures. Some cases show the unpreparedness of digital platforms in managing and protecting users' personal data. Many platforms are not fully prepared to anticipate cyber threats, such as data leaks due to hacking or negligence in data management. The weak verification system in freelance job vacancies is one real example. Many platforms do not conduct adequate background checks or verification of the person offering the job. This risks leading to fraud, where the personal data of job seekers can fall into the wrong hands. The level of compliance of digital platforms with the provisions of the PDP Law varies. Large platforms are usually already strictly regulated, while small or unknown platforms often don't have adequate data protection systems in place. This gap creates loopholes that allow the misuse of personal data by irresponsible parties.

Law enforcement against violations of the PDP Law is also constrained. Although the PDP Law stipulates administrative sanctions for data controllers who violate, these sanctions often do not have a deterrent effect. The lack of supervision from the authorities, such as the Ministry of Communication and Information Technology or the Personal Data Protection Authority, has also exacerbated the situation (Sinaga & Putri, 2020). Without strict enforcement, the obligation of digital platforms to protect personal data becomes suboptimal, thereby increasing the risk of data leakage or fraud. The legal responsibility of digital platforms in protecting personal data includes technical obligations as well as commitments to maintain user trust (Sulistianingsih et al., 2023). More serious efforts are needed to prevent the misuse of personal data, such as strengthening regulations, stricter supervision, and educating users about the importance of protecting personal data in the digital world.

Application of the PDP Law in the Cyber Prime Case

The application of the Personal Data Protection Law (PDP Law) in the context of cybercrime is very relevant to protect personal data from evolving threats. The PDP Law provides a clear legal basis for individuals to prosecute perpetrators of crimes that damage their privacy. In the context of cyber crime, the PDP Law not only regulates the protection of personal data, but also provides certain rights to data owners, such as the right to access, correct, and delete

personal data that has been collected by third parties Article 27 of the PDP Law provides a legal basis to prosecute data controllers who are negligent in managing personal data, such as in the case of data leakage or data misuse by irresponsible parties. In this case, data controllers who do not carry out their obligations properly can be subject to administrative sanctions, such as fines, or even criminal sanctions if proven to have committed acts that are detrimental to the data owner. This sanction aims to provide a deterrent effect to data controllers who do not comply with applicable rules (Mardiana & Arsanti, 2023).

However, the implementation of the PDP Law in cybercrime cases in Indonesia still faces a number of challenges. One of the main challenges is the low awareness of the public regarding their rights related to personal data protection. Many internet users are unaware that they have the right to control the personal data they share on digital platforms. This is often used by irresponsible parties to commit fraud or data theft. The lack of coordination between agencies is also an obstacle in the implementation of the PDP Law in cybercrime cases. In many cases, authorized agencies such as Ministry of Communication and Information Technology or the Personal Data Protection Authority do not have an effective mechanism to overcome and crack down on violations related to personal data protection. Better coordination between government agencies and digital platforms is urgently needed to ensure that the PDP Law is implemented consistently and effectively in preventing cybercrime.

The lack of coordination between agencies is also an obstacle in the implementation of the PDP Law in cybercrime cases. In many cases, authorized agencies such as Ministry of Communication and Information Technology or the Personal Data Protection Authority do not have an effective mechanism to overcome and crack down on violations related to personal data protection. Better coordination between government agencies and platform digital is urgently needed to ensure that the PDP Law is implemented consistently and effectively in preventing cybercrime (Fikri & Rusdiana, 2023).

Cyber crime cases involving freelance job vacancy fraud increasingly show how vulnerable job seekers' personal data is in the digital world. Many criminals take advantage of the victim's ignorance to access personal data which is then misused. For example, job scams often ask potential workers to provide sensitive personal information, such as bank account numbers or identity documents, under the pretext of a recruitment or payment process. The data that has been provided is then used for interests that are detrimental to the victim. In some cases, even if the perpetrators of cybercrimes are successfully caught, the long and complex legal process often slows down the delivery of justice to the victims. Therefore, it is important for the public to be more vigilant and understand the importance of personal data protection.

In addition, digital platforms must also play an active role in ensuring that they meet their legal obligations regarding the protection of users' personal data. The implementation of the PDP Law in handling cyber crime cases requires strengthening the legal system and stricter enforcement of violations that occur. The establishment of a stronger Personal Data Protection Authority and increased public awareness of personal data protection will accelerate efforts to reduce the number of cybercrimes in Indonesia (Matheus & Gunadi, 2024). Strict law enforcement against cyber crime perpetrators, along with the obligation of digital platforms to protect personal data, will create a safer and more reliable digital ecosystem.

CONCLUSION

Based on the results of the research, the legal responsibility of digital platforms in protecting personal data includes the obligation to maintain transparency, obtain the consent of the data owner, and prevent data leakage. However, many platforms are still unprepared to deal with cyber threats, such as negligence in job verification that is vulnerable to fraud. The implementation of the Personal Data Protection Law in cybercrime cases provides a strong legal basis for prosecuting perpetrators and enforcing administrative sanctions, although its

implementation is still limited due to low public awareness and lack of coordination between agencies. Therefore, there is a need to increase public education, strengthen the technical capacity of law enforcement officials, and better collaboration between regulators, digital service providers, and the public to ensure more effective protection of personal data in the future.

REFERENCE

Djafar, W., & Santoso, M. J. (2019). PERLINDUNGAN DATA PRIBADI: Konsep, Instrumen, dan Prinsipnya. Lembaga Studi dan Advokasi Masyarakat (ELSAM).

Fikri, M., & Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia. Ganesha Law Review, 5(1), 39–57.

Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (Ruu) Perlindungan Data Pribadi. Jurnal Hukum, 37(2), 119–133.

Mardiana, N., & Arsanti, M. (2023). URGENSI PERLINDUNGAN DATA PRIBADI DALAM PRESPEKTIF HAK ASASI MANUSIA. Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia, 5(1), 16–23. https://doi.org/10.52005/rechten.v5i1.108

Matheus, J. (2021). E-Arbitration: Digitization Of Business Dispute Resolution Pada Sektor E-Commerce Dalam Menyongsong Era Industri 4.0 Di Tengah Pandemi Covid-19. Lex Renaissance, 6(4), 692–704.

Matheus, J., & Gunadi, A. (2024). Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital: Kajian Perbandingan Dengan KPPU. JUSTISI, 10(1), 20–35.

Palinggi, S., & Limbongan, E. C. (2020). Pengaruh Internet Terhadap Industri Ecommerce dan Regulasi Perlindungan Data Pribadi Pelanggan di Indonesia. Semnas Ristek (Seminar Nasional Riset Dan Inovasi Teknologi), 225–232. https://doi.org/https://doi.org/10.30998/semnasristek.v4i1.2543

Sinaga, E. M. C., & Putri, M. C. (2020). Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0. Jurnal Rechtsvinding, 9(2), 237–256. https://doi.org/http://dx.doi.org/10.33331/rechtsvinding.v9i2.428

Sulistianingsih, D., Ihwan, M., Setiawan, A., & Prabowo, M. S. (2023). TATA KELOLA PERLINDUNGAN DATA PRIBADI DI ERA METAVERSE (TELAAH YURIDIS UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI). Masalah-Masalah Hukum, 52(1), 97–106. https://doi.org/10.14710/mmh.52.1.2023.97-106.