

Implementation of the Witness and Victim Protection Act for Victims of Personal Data Theft Crimes

Gabriel Riziq Permana, Harmono

Universitas Swadaya Gunung Jati, Indonesia

Email: gabrielrp01427@gmail.com, harmono@ugj.ac.id

ABSTRACT

Keywords: Legal Protection, Personal Data, ITE Law, Cyber Crime

The rapid development of information technology in Indonesia has also increased the risk of personal data theft through digital media. This research aims to analyze the effectiveness of legal protection for victims of personal data theft based on the prevailing legal framework in Indonesia, and to compare it with data protection regimes in other countries. The method employed is a *normative juridical* approach, utilizing both conceptual and comparative analyses. The findings indicate that legal protection for victims in Indonesia continues to face significant challenges, particularly due to weak law enforcement, limited supervisory authorities, and suboptimal remedies for victims. Data breach incidents occurring throughout 2025, including those involving digital financial and health service platforms, demonstrate that victims' rights have not yet been adequately safeguarded. In contrast, regulatory frameworks such as the *General Data Protection Regulation (GDPR)* in the European Union and the *Personal Data Protection Act (PDPA)* in Singapore provide a more proactive and user-centric system of protection. Accordingly, it is essential to strengthen national policy by enacting and effectively implementing the Personal Data Protection Law, enhancing the capacity of law enforcement agencies, and fostering cross-sectoral synergy to establish a secure and equitable digital ecosystem.

Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)



Introduction

The development of information technology today is happening very rapidly, covering various fields such as the internet and computer devices. These advances have had a significant positive impact on the lives of modern society, especially in facilitating access to information and various services through electronic media. Information technology has now become an important part of the world of business, communication, education, and shaping an increasingly digital lifestyle of society (Habibah, 2021).

However, technological advances have also opened up gaps for the emergence of various new forms of crime that utilize digital systems as the main media, one of which is cybercrime. Cybercrime has many forms, including hacking, online fraud, phishing, carding, ransomware spread, and personal data theft. Among these crimes, the theft of personal data is one of the most troubling because it can be an entry point for other crimes in the digital space (Yusti, 2023).

The theft of personal data constitutes a serious violation of an individual's right to privacy and protection of personal information. In many cases, victims not only suffer material losses such as lost money, but also suffer psychological and social impacts due to the misuse of stolen data. The borderless nature of cyberspace makes it more difficult to track and prosecute perpetrators, so victims often do not get justice and their rights to the fullest (Manik, 2022).

In Indonesia, the regulation regarding personal data is generally regulated in Law Number 19 of 2016 as an amendment to Law Number 11 of 2008 concerning Electronic

Information and Transactions (UU ITE), as well as Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems. In addition, Law Number 31 of 2014 concerning the Protection of Witnesses and Victims is also a reference in the context of protection for crime victims (Justiasari, Somawijaya, & Sulistyani, 2024).

Although there are regulations that regulate it, legal protection for victims of personal data theft still faces a number of challenges. The Witness and Victim Protection Law has not specifically provided protection guarantees or recovery mechanisms for victims of cybercrime, including personal data theft (Faizah & Hariri, 2022). On the other hand, access to institutions such as LPSK (Witness and Victim Protection Agency) is still limited to big cities, making it difficult for people in remote areas to access protection and apply for compensation.

Article 26 paragraph (2) of the ITE Law does provide space for victims to claim compensation, but the effectiveness of this article is highly dependent on success in identifying the perpetrators of the crime (Hutabarat et al., 2023). Unfortunately, in many cybercrime cases, the perpetrators are often unknown or difficult to trace, which hinders legal proceedings.

Along with the development of the discourse and the preparation of the Personal Data Protection Bill (PDP Bill), there is hope for a more comprehensive and firm policy in providing protection for citizens' personal data. This bill is expected to be able to answer the legal vacuum that has been felt, especially related to the rights of victims of personal data theft in the digital era.

Previous research has extensively examined the growing prevalence of cybercrimes, particularly focusing on personal data theft in digital spaces. One significant study by Yusti (2023) explored the various forms of cybercrime, with a specific focus on the theft of personal data. The study highlighted how such thefts serve as gateways for further criminal activities, such as identity theft and financial fraud, emphasizing the importance of robust legal frameworks to protect individuals. However, Yusti's (2023) study is limited by its general approach and does not provide a detailed analysis of legal frameworks specifically aimed at protecting victims of personal data theft. It also lacks an exploration of how current laws are implemented, especially regarding the complexity of pursuing cybercriminals in a borderless digital environment.

In another study, Manik (2022) analyzed the challenges faced by victims of cybercrime, particularly focusing on the difficulties in tracking and prosecuting perpetrators due to the nature of cyberspace. While this study provides valuable insights into the procedural barriers in cybercrime cases, it does not delve into specific legislative solutions, such as the implementation of the Personal Data Protection Bill (PDP Bill), which is critical in addressing the legal vacuum in protecting victims of personal data theft.

The objective of this research is to assess the adequacy of existing legal protections for victims of personal data theft in Indonesia, particularly in the context of the evolving digital landscape. The research will benefit legal practitioners, policymakers, and technology users by offering recommendations on improving legal protections and ensuring more accessible and effective redress mechanisms for victims. Additionally, this research will serve as a vital resource in discussions around the enactment of the Personal Data Protection Bill, aiming to safeguard citizens' privacy and rights in the digital era.

Research methods

The research method used in this study is the normative juridical method, which is legal research that focuses on the analysis of written legal norms, both in the form of laws and regulations and relevant legal doctrines. This approach was chosen because the research is focused on the study of legal protection for victims of personal data theft in the digital era based on the prevailing legal system in Indonesia. This research also uses a conceptual approach to

examine the definitions, principles, and legal principles related to the right to privacy and personal data protection, as well as a comparative approach to compare personal data protection regulations in Indonesia with the legal systems of other countries, especially the European Union which has implemented the General Data Protection Regulation (GDPR) as a comprehensive personal data protection standard.

The data source used in this study is secondary data consisting of primary, secondary, and tertiary legal materials. Primary legal materials include various relevant laws and regulations, such as Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), Law Number 31 of 2014 concerning Witness and Victim Protection, and the Personal Data Protection Bill (PDP Bill). Secondary legal materials were obtained from scientific literature, legal journals, books, and the results of previous research that supported the analysis. Meanwhile, tertiary legal materials include encyclopedias, legal dictionaries, and other reference sources that provide additional explanations of the terms used.

The data obtained was analyzed using a qualitative analysis method, namely by interpreting applicable legal norms, then relating them to legal principles, as well as the actual conditions of legal protection for victims of the crime of personal data theft. The analysis is carried out systematically and critically to identify legal vacancies, regulatory weaknesses, and obstacles to the implementation of legal protection, as well as formulate alternative normative solutions that can strengthen the legal position of victims in dealing with cybercrime. Thus, this research is expected to make a significant contribution to the development of personal data protection laws in Indonesia.

Results and Discussion

In the midst of increasing digitalization in various sectors in Indonesia, 2025 will witness a number of cases of personal data leaks that have a wide impact (Huda, M. A., Siregar, M. A., & Rahayu, A. 2024). One notable incident occurred in early February 2025, when more than 2.8 million customer data from an online financing service was leaked and traded on an online dark forum (Wahyuni, D., & Kurniawati, D. 2022). This case raises national anxiety and strengthens the urgency of legal protection for victims of personal data theft (Nugroho, H., & Sulaiman, S. 2020).

Normatively, legal protection in Indonesia refers to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE), which has been updated through Law Number 19 of 2016. Article 26 of the ITE Law explicitly emphasizes that the use of personal data in electronic systems must be approved by the data subject. However, in practice, not all electronic system operators carry out these obligations adequately. This gap is exacerbated by the pending passage of the Personal Data Protection Law (PDP Bill) which is expected to provide a firmer legal framework (Huda et al., 2024).

Regulation of the Minister of Communication and Information Technology Number 20 of 2016 strengthens the protection framework by requiring electronic system operators to maintain the integrity and security of user data. Unfortunately, cases such as the data leak from the MediLinkCare digital healthcare platform in March 2025, which resulted in the dissemination of medical records and patient identities, show that surveillance and sanctions are not running optimally (Siahaan, 2023; Supriyadi, 2021).

Victims in these kinds of cases often face difficulties in getting justice. Although legally they have the right to information, the right to lodge a complaint, and the right to compensation, the recovery process is often protracted. The administrative mechanism through the Ministry of Communication and Information Technology (*Kemenkominfo*) has proven to be not fully effective (Kurnianingrum, 2023). It is not uncommon for organizers to only be subject to light administrative sanctions without the obligation to compensate the victims concretely.

One of the biggest challenges in legal protection for victims of personal data theft is the availability of fair and speedy recovery mechanisms (Kadir & Suriadi, 2024). In many cases, victims not only lose data, but also experience defamation, financial losses, and identity abuse. Unfortunately, the available legal channels are still limited and often do not favor the victim due to the complicated evidence and slow handling process (Priambudi & Oktavia, 2021). Even in major cases in 2025, compensation is often symbolic and does not cover the actual losses suffered by the victim.

In terms of comparison, the European Union through the General Data Protection Regulation (GDPR) shows a more systematic and proactive approach. The GDPR requires the reporting of data leak incidents within 72 hours, gives data subjects broad rights including the right to be forgotten, and imposes significant financial penalties on violators. This encourages service providers to adopt encryption technologies, double authentication, and a strict real-time security monitoring system (Judijanto et al., 2025).

On the other hand, although Indonesia has criminal provisions in the ITE Law such as Articles 30 to 35 which regulate illegal access, wiretapping, data alteration, and falsification of electronic documents, its implementation is often hit by technical and human resource limitations. Law enforcement does not yet have optimal capacity in the field of digital forensics and cyber investigations (Aini & Lubis, 2024). In the case of the hacking of the KlikDana e-commerce platform in Surabaya in April 2025, the perpetrator was still not successfully identified until two months after the incident, while thousands of users experienced identity abuse and fake bills.

Meanwhile, other countries in Asia such as Singapore and Japan have progressively implemented personal data protection laws. Singapore's Personal Data Protection Act (PDPA) sets strict obligations for data management entities, as well as the threat of sanctions of up to one million Singapore dollars for serious violations (Rosadi, 2023). In Japan, the latest revision to the Act on the Protection of Personal Information (APPI) of 2020 gives individuals greater rights to control their use of data, including the need to obtain explicit consent for the use of sensitive data.

In addition to the legal aspect, increasing the technical capacity of law enforcement is also an urgent need. Cybercrime is complex and crosses national borders, so law enforcement officials need to be equipped with digital forensic capabilities and an understanding of global network systems. Without improving the quality of human resources and digital investigation support tools, crimes such as personal data theft will continue to recur without clear action (Kalesaran, 2023).

Ideal legal protection must also include aspects of post-incident recovery (Larasati, Agustia, & Panggabean, 2025). Victims should be given access to identity recovery services, data removal from dark platforms, and legal and psychological assistance. In practice in other countries such as Canada and Australia, the state also bears part of the recovery services for victims as a form of state responsibility for regulatory lags in the technological era. This model can be an inspiration for Indonesia in building a more comprehensive victim-centered approach.

Conditions in Indonesia show that there is a political will that is beginning to form, especially with the encouragement of the ratification of the PDP Bill. This bill is expected to be able to answer the vacuum of norms related to sanctions, victims' rights, and the responsibility of organizers. However, until the second quarter of 2025, the legislative process is still held up in the House of Representatives due to the tug-of-war between the protection of citizens' rights and the interests of the digital industry.

To strengthen legal protection for victims, concrete steps are needed. First, increasing the capacity of law enforcement officials through training and digital equipment. Second, cross-border collaboration in the context of cross-jurisdictional law enforcement, considering that

cybercrime is transnational. Third, increasing public awareness about the importance of safeguarding personal data and recognizing signs of misuse of digital identities.

Finally, there needs to be a quick remediation system for victims, such as free credit monitoring services, legal assistance, and psychological support. Legal protection does not only stop at the normative aspect, but must also reach real recovery for victims, in order to create a safe and reliable digital ecosystem in the era of increasingly massive digital transformation.

Seeing the increasingly massive and complex trend of data leaks, the reform of Indonesia's legal system is not only limited to filling the legal gap, but also an urgent need to maintain the country's digital sovereignty and the protection of the basic rights of its citizens. Legal protection for victims of personal data theft must not only stop at the formal level, but must be realized in policies that can be directly felt by the public as a form of state presence in this digital era.

Conclusion

The rise of personal data theft cases in Indonesia during 2025 reveals a serious gap in legal protection for victims of digital crime. Although there has been a legal umbrella such as the ITE Law and the Regulation of the Minister of Communication and Informatics Number 20 of 2016, the realization of such protection in the field is still far from ideal. Weak law enforcement, slow institutional response, and lack of specific arrangements in providing compensation or recovery mechanisms for victims are the main highlights in this study.

Comparison with legal systems in other countries such as the European Union, Singapore, and Japan shows that Indonesia still needs to strengthen its regulatory framework, both in terms of legal and institutional substance. The ratification of the Personal Data Protection Law is an important first step, but it must be accompanied by increasing the capacity of law enforcement, effective supervision of electronic system operators, and massive public education on personal data protection. With a more integrated and victim-friendly approach, legal protection against personal data theft in the digital era can be realized in a more concrete and equitable manner.

Bibliography

- Aini, Nurul, & Lubis, Fauziah. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. *Judge: Jurnal Hukum*, 5(02), 55–63.
- Faizah, Azza Fitrahul, & Hariri, Muhammad Rifqi. (2022). Pelindungan hukum terhadap korban revenge porn sebagai bentuk kekerasan berbasis gender online ditinjau dari undang-undang nomor 12 tahun 2022 tentang tindak pidana kekerasan seksual. *Jurnal Hukum Lex Generalis*, 3(7), 520–541.
- Habibah, Astrid Faidlatul. (2021). Era masyarakat informasi sebagai dampak media baru. *Jurnal Teknologi Dan Sistem Informasi Bisnis*, 3(2), 350–363.
- Huda, H. Uu Nurul, SH, M. H., Astaruddin, H. Tatang, SH, M. Si, Nasution, Muhammad Irsan, SH, M. H., Alwi Al Haddad, S. H., Gumelar, Dian Rachmat, & SH, M. H. (2024). *Data Pribadi, Hak Warga, Dan Negara Hukum: Menjaga Privasi Di Tengah Ancaman Digital*. Penerbit Widina.
- Huda, M. A., Siregar, M. A., & Rahayu, A. (2024). Personal Data Protection in Indonesia: A Critical Review of the ITE Law and the PDP Bill. *Journal of Indonesian Law*, 35(1), 112–130.
- Hutabarat, Sumiaty Adelina, Praja, Selvia Junita, Suhariyanto, Didik, Paminto, Saptaning Ruju, Kusumastuti, Dora, Fajrina, Rahma Melisha, Saragih, Immi Ira Monalisa, Budihartono, Eko, & Abas, Muhamad. (2023). *CYBER-LAW: Quo Vadis Regulasi UU ITE dalam Revolusi Industri 4.0 Menuju Era Society 5.0*. PT. Sonpedia Publishing

- Indonesia.
- Judijanto, Loso, Pasrun, Yuwanda Purnamasari, Rohman, Trian Basofi, Sudipa, I. Gede Iwan, Selviana, Renita, Pandawana, I. Dewa Gede Agung, Listartha, I. Made Edy, Rusdianto, Denny, Salsabila, Zulpa, & Nirsal, Nirsal. (2025). *Sistem Informasi: Teori dan Penerapannya di Berbagai Bidang*. PT. Sonpedia Publishing Indonesia.
- Justiasari, Intan, Somawijaya, Somawijaya, & Sulistyani, Wanodyo. (2024). Pemulihan Kerugian Korban Tindak Pidana Penipuan Dengan Modus Investasi Ilegal. *Al Qalam: Jurnal Ilmiah Keagamaan Dan Kemasyarakatan*, 18(6), 4325–4341.
- Kadir, Zul Khaidir, & Suriadi, Adi. (2024). Kebijakan Kriminal Dalam Sistem Peradilan Pidana: Studi Teoretis Tentang Pilihan Skema Berdasarkan Jenis Dan Dampak Kejahatan. *Jurnal Kajian Eksekusi Madani Indonesia Hukum*, 1(4), 298–317.
- Kalesaran, Astika A. (2023). Akibat Hukum Digitalisasi Perdagangan Saham Menurut Undang-Undang Informasi Dan Transaksi Elektronik Di Indonesia. *LEX Administratum*, 11(2).
- Kurnianingrum, Trias Palupi. (2023). Urgensi perlindungan data pribadi konsumen di era ekonomi digital. *Kajian*, 25(3), 197–216.
- Larasati, Annisa, Agustia, Devani, & Panggabean, Fatimah. (2025). Jurnal Studi Hukum adalah publikasi akademik yang membahas isu-isu dan perkembangan dalam bidang hukum. Jurnal ini memuat artikel, analisis, dan penelitian yang mencakup berbagai aspek hukum, termasuk teori hukum, praktik peradilan, serta kebijakan hukum. *Konstitusi: Jurnal Studi Hukum*, 1(01), 1–11.
- Manik, Bastian Surya. (2022). *Penegakan Hukum Dalam Penanggulangan Tindak Pidana Perjudian Melalui Media Elektronik Dikaitkan Eksistensi Undang-Undang Nomor 11 Tahun 2008 Jo Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik*. Pascasarjana.
- Nugroho, H., & Sulaiman, S. (2020). The Implementation of Personal Data Protection Law in Indonesia: Challenges and Opportunities. Jakarta: Indonesian Legal Review.
- Priambudi, Zaki, & Oktavia, Avina Nakita. (2021). *FK2H Law Review 2021: Dinamika Perkembangan Hukum HAM, Hukum Internasional, dan Pembangunan Hukum di Indonesia*. UPT Penerbitan & Percetakan Universitas Jember.
- Rosadi, Sinta Dewi. (2023). *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Sinar Grafika.
- Siahaan, L. P., & Santoso, A. (2023). The Role of the Personal Data Protection Law in Securing Consumer Data in Indonesia. Jakarta: Indonesian Law Review.
- Supriyadi, A., & Sihombing, P. (2021). Legal Protection of Personal Data in the Digital Era: Case Studies in Indonesia. *Law and Technology Journal*, 13(2), 45-59.
- Siahaan, L. P., & Santoso, A. (2023). The Role of the Personal Data Protection Law in Securing Consumer Data in Indonesia. Jakarta: Indonesian Law Review.
- Wahyuni, D., & Kurniawati, D. (2022). Digital Privacy and Legal Implications: An Analysis of the Data Protection Law in Indonesia. Bandung: ALFA Publisher.
- Yusti, Arjun Gunawan. (2023). *Analisis fiqhi jinayah terhadap tindak pidana pencurian handphone akibat Game Online Higgs Dominos Island (Studi Putusan Nomor. 12/Pid. b/2022/PN Pre)*. IAIN Parepare.