DOI: 10.46924/jihk.v6i2.225

Personal Data Protection Policies and Their Impact on Victims of Cybercrime

Vicky Ibrahim[1], Yeti S. Hasan[2], Parmin Ishak[3]*

[1,2,3]Law Faculty, Universitas Ichsan Gorontalo Utara, Indonesia

Correspondence

Parmin Ishak, Universitas Ichsan Gorontalo Utara, Indonesia, Jl. Drs. Achmad Nadjamuddin, Limba U Dua, Kota Sel., Kota Gorontalo, Gorontalo 96138, e-mail: parminishak72@gmail.com

How to cite

Ibrahim, Vicky., Hasan, Yeti S., and Ishak, Parmin. 2025. "Personal Data Protection Policies and Their Impact on Victims of Cybercrime". *Jurnal Ilmu Hukum Kyadiren* 6 (2), 13-25. https://doi.org/10.46924/jihk.v6i2.225

Original Article

Abstract

This study aims to analyze personal data protection policies in Indonesia and their impact on cybercrime victims, with a specific focus on their implementation in Gorontalo Province. In the digital era, personal data has become a valuable asset but remains highly susceptible to various forms of misuse. Law No. 27 of 2022 on Personal Data Protection was enacted to safeguard individual privacy rights. However, its implementation continues to face challenges, including low digital literacy, insufficient infrastructure, and weaknesses in law enforcement. The study also highlights the significant effects of cybercrime on victims, such as financial losses, psychological trauma, and substantial social consequences. Addressing these issues requires a comprehensive approach and enhanced international cooperation. This research recommends improving digital literacy, strengthening technological infrastructure, and formulating more specific local regulations in Gorontalo to enhance personal data protection.

Keywords: *Victim Protection; Protection of Personal Data; Cybercrime*

Abstrak

Penelitian ini bertujuan untuk memahami bagaimana kebijakan perlindungan data pribadi di Indonesia diterapkan dan bagaimana dampaknya terhadap korban kejahatan cyber dengan fokus khusus pada implementasinya di provinsi gorontalo. Di era digital ini, data pribadi menjadi aset yang sangat berharga sekaligus rentan terhadap berbagai bentuk pelanggaran. Undang-Undang Nomor 27 Tahun 2022 tentang perlindungan data pribadi telah disahkan sebagai upaya untuk melindungi hak privasi individu, namun implementasinya masih menghadapi berbagai tantangan seperti rendahnya literasi digital, infrastruktur yang belum memadai dan kelemahan dalam penegakan hukum. Penelitian ini juga mengungkapkan bahwa kejahatan cyber memiliki dampak yang sangat signifikan terhadap korban, mencakup kerugian finansial, trauma psikologis dan dampak sosial yang mendalam. Untuk mengatasi tantangan tersebut, diperlukan pendekatan yang holistik dan kerjasama internasional yang lebih kuat. Penelitian ini merekomendasikan peningkatan literasi digital, pengembangan infrastruktur teknologi yang lebih kuat dan penyusunan peratura daerah yang lebih spesifik di gorontalo untuk memperkuat perlindungan data pribadi.

Kata kunci: *Perlindungan Korban, Perlindungan Data Pribadi, Kejahatan Siber*

1. INTRODUCTION

Technological advancements have significantly transformed nearly every aspect of human life, from communication and increased information access to innovations in health, education, and business sectors.[1] Technology has become a catalyst for unprecedented progress and efficiency.[2] However, alongside these substantial benefits, technological advancements also introduce new and complex challenges, including the escalating risk and frequency of cybercrime. Such crimes not only result in financial losses but also raise critical concerns regarding privacy and personal data protection.[3]

In 2019, Gorontalo Province recorded at least 20 cases of cybercrime, underscoring an urgent need to enhance cybersecurity and data protection measures. This issue became even more pressing in 2023, when a report from DetikSulsel revealed that substantial amounts of public data from Gorontalo had been leaked on the internet.[4] This situation underscores the vulnerabilities in digital infrastructure and shortcomings in personal data protection practices. Despite ongoing efforts to improve data security and protection, significant gaps remain, allowing data breaches and other cybercrimes to persist. These issues not only lead to material losses for individuals and institutions but also erode public trust in digital technology.[5]

Law Number 27 of 2022 on Personal Data Protection defines personal data as information about individuals that can be identified directly or indirectly, either independently or in combination with other information, through electronic or non-electronic systems. According to Article 1, Clause 2 of the PDP Law, personal data protection encompasses all measures taken to safeguard personal data during the data processing cycle, with the objective of ensuring the constitutional rights of individuals whose data is being processed.[6]

On the other hand, cybercrime refers to criminal activities conducted via the internet or through computers connected to internet networks. This category of crime includes actions such as data theft, account hacking, system sabotage, the dissemination of viruses, and other harmful activities. Cybercrime can have far-reaching and severe consequences

---

1 Gema Bangsawan, "Kebijakan Akselerasi Transformasi Digital Di Indonesia: Peluang Dan Tantangan Untuk Pengembangan Ekonomi Kreatif," *Jurnal Studi Kebijakan Publik* 2, no. 1 (2023): 27–40, https://doi.org/10.21787/jskp.2.2023.27-40.

2 Jupri Jupri et al., "A Model of Legal Culture for Prevention of Money Politics Through Social Media Strategies for Facing Simultaneous Elections in 2024 Gorontalo Province," *Jurnal Hukum Volkgeist* 8, no. 1 (2023): 123–32, https://www.jurnal-umbuton.ac.id/index.php/Volkgeist/article/view/4356.

3 Hari Sutra Disemadi et al., "Perlindungan Data Pribadi Di Era Digital: Mengapa Kita Perlu Peduli?," *Sang Sewagati Journal* 1, no. 2 (2023): 67–90, https://doi.org/10.37253/sasenal.v1i2.8579.

4 Apris Nawu, "Data Kependudukan Warga Gorontalo Bocor Di Internet, Pelaku Petugas Puskesmas," Detiksulsel, 2023, https://www.detik.com/sulsel/berita/d-6921091/data-kependudukan-warga-gorontalo-bocor-di-internet-pelaku-petugas-puskesmas.

5 L. Alfies Sihombing and Yeni Nuraeni, "Norms and Ethics in Criminal Justice: Assessing Contemporary Legal Policy," *Jurnal Info Sains: Informatika Dan Sains* 13, no. 3 (2023): 1088–1099, https://ejournal.seaninstitute.or.id/index.php/InfoSains/article/view/3693.

6 Republik Indonesia, "Undang-Undang Nomor 27 Pelindungan Data Pribadi" (2022), https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022.

for victims, society, and the economy. Beyond financial losses, cybercrime can tarnish reputations, disrupt essential services, and inflict psychological and emotional harm on victims.[7]

Several previous studies have highlighted the critical need for robust regulations to safeguard personal data. Firdaus criticized the inability of existing regulations to prevent data breaches and emphasized the necessity for stricter and more collaborative law enforcement among relevant stakeholders.[8] Similarly, Kholiviya underscored the urgent need to strengthen regulatory frameworks, enhance law enforcement efforts, and raise public awareness about personal data protection.[9]

Research by Hariyono and Simangunsong stressed the importance of adopting a stronger and more integrated approach to law enforcement while simultaneously increasing public awareness to effectively combat phishing-related cybercrimes.[10] Widianingrum et al. argued that addressing cybercrime effectively requires improvements in digital education and literacy, the development of technical capacity, and inter-institutional collaboration. Additionally, they highlighted the importance of revising regulations to ensure they remain responsive to evolving cybercrime challenges.[11] A juridical study by Greece and Ilmih further emphasized the need for robust cyber-adoption strategies and international collaboration to address the growing threats of cybercrime and to protect personal data in the increasingly digitized era.[12]

This study focuses on the experiences and impacts of cybercrime on victims, enabling a more nuanced analysis of how personal data protection policies function not only as preventive measures but also as tools for victim recovery. By adopting a victim-centered approach, the research seeks to uncover gaps in current support systems and provide recommendations for enhancing services and resources for those affected.

The urgency of this study lies in addressing the need for robust personal data protection by evaluating existing policies, identifying deficiencies, and proposing improvements to better support cybercrime victims. It also aims to increase public awareness and education about the importance of data security while ensuring that personal

---

7 Russel Butarbutar, "Kejahatan Siber Terhadap Individu: Jenis , Analisis , Dan Perkembangannya," *Technology and Economiacs Law Journal* 2, no. 2 (2023): 297–316, https://doi.org/10.21143/TELJ.vol2.no2.1043.

8 Indriana Firdaus, "Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan," *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia* 4, no. 2 (2022): 23–31, https://doi.org/10.52005/rechten.v4i2.98.

9 Hasna Kholiviya, "Perlindungan Hukum Terhadap Korban Pencurian Data Pribadi Dalam Kasus Tindak Pidana Mayantara (Cyber Crime)" (Universitas Islam Sultan Agung Semarang, 2021), https://repository.unissula.ac.id/24642/.

10 Akbar Galih Hariyono and Frans Simangunsong, "Perlindungan Hukum Korban Pencurian Data Pribadi (Phishing Cybercrime) Dalam Perspektif Kriminologi," *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 3, no. 1 (2023): 1–12, https://doi.org/10.53363/bureau.v3i1.191.

11 Afifah Rizqy Widianingrum, "Analisis Implementasi Kebijakan Hukum Terhadap Penanganan Kejahatan Siber Di Era Digital," *Journal Iuris Scientia* 2, no. 2 (2024): 90–102, https://doi.org/10.62263/jis.v2i2.40.

12 Farhan A Yunani and Andi Aina Ilmih, "Kajian Yuridis Kejahatan Lintas Negara Berkaitan Dengan Perlindungan Data Pribadi," *Media Hukum Indonesia* 2, no. 3 (2024): 586–92, https://ojs.daarulhuda.or.id/index.php/MHI/article/view/660.

data protection and cybersecurity measures in Gorontalo Province align with international standards.

Given this context, the objectives of the study are to analyze personal data protection policies in Gorontalo, identify gaps in their implementation, and evaluate the direct impacts of cybercrime on victims. Using a comprehensive approach, the research examines challenges in law enforcement, the level of public awareness and understanding of cybercrime risks, and the adequacy of technological infrastructure supporting personal data protection efforts.

2. RESEARCH METHODOLOGY

This study employs a normative legal research design using a normative juridical approach to critically analyze personal data protection policies and their impact on cybercrime victims. The objective is to gain a comprehensive understanding of personal data protection policies, identify gaps in their implementation, and evaluate the direct impacts of cybercrime on victims. Normative legal research aims to provide a legal framework that assesses whether an event aligns with or contravenes the law and determines how such events should be legally addressed and regulated.[13] In addition, the normative juridical approach as a legal study based primarily on library research or secondary data, involving an examination of legal regulations and literature relevant to the research topic.[14]

The data utilized in this study is secondary data, which includes primary legal materials such as the 1945 Constitution of the Republic of Indonesia, Law Number 27 of 2022 on Personal Data Protection, the Indonesian Penal Code (KUHP), and related government regulations. In addition, secondary legal materials, including the opinions of criminal law experts from literature, journals, and articles (both printed and electronic), are also used. The data obtained through the literature review is analyzed using a descriptive approach. This method not only describes the collected data but also employs triangulation to verify and compare secondary data, ensuring consistency and accuracy across various sources. The result is the formulation of provisional conclusions or valid research findings.

3. RESEARCH RESULT AND DISCUSSION

3.1. Personal Data Protection in the Digital Era: Challenges and Strategies

The protection of personal data in the digital era has become a critical concern, driven by the pervasive use of information and communication technology across various aspects of life. In Indonesia, this issue has garnered significant attention with the enactment of Law Number 27 of 2022 on Personal Data Protection (PDP Law). This legislation serves as the legal framework for safeguarding individual rights over personal data and establishes regulations on how such data is collected, stored, used, and processed by relevant parties.

---

13 M Fajar and A Yulianto, *Dualisme Penelitian Hukum Dan Empiris* (Jakarta: Pustaka Pelajar, 2010).

14 Soerjono Soekanto and Sri Mamudji, *Penelitian Hukum Normatif : Suatu Tujuan Singkat* (Jakarta: PT.Raja Grafindo Persada, 2003).

The PDP Law underscores that every individual has the right to personal data protection, encompassing the right to privacy, the right to access and rectify personal data, and the right to object to the processing of personal data deemed harmful. Additionally, the law imposes specific obligations on data controllers and processors to uphold confidentiality and ensure the integrity and security of personal data. These responsibilities include implementing appropriate technical and organizational measures to protect personal data from unauthorized access or disclosure and to prevent accidental loss or damage.

In Gorontalo, although there are no specific regional regulations (Peraturan Daerah or Perda) addressing personal data protection, several existing regulations can be associated with efforts to safeguard personal data in the digital era. While not explicitly targeting personal data protection, these regulations are relevant within the context of information and communication technology governance, data management, and technology-based public services. For instance, Gorontalo has implemented regulations supporting the adoption of an electronic-based government system (Sistem Pemerintahan Berbasis Elektronik or SPBE). Through this framework, the regional government aims to integrate information technology into various public services, with personal data security forming a critical component, particularly in managing data collected via electronic platforms.

Under the SPBE framework, the regional government bears the responsibility of ensuring that personal data managed within this system is secure and protected from potential threats. Additionally, regional consumer protection policies in Gorontalo also emphasize the importance of safeguarding personal data in interactions between consumers and businesses. Protecting consumer data is essential, as mishandled personal data can be exploited if not properly managed.

Despite these efforts, the implementation of Law No. 27 of 2022 on Personal Data Protection (PDP Law) in Gorontalo faces significant challenges. A key issue lies in the readiness of technological infrastructure and human resources. While SPBE and related policies have been introduced, low digital literacy among the public and government officials remains a significant barrier to effective implementation. A lack of awareness regarding the importance of personal data protection often results in non-compliance with existing regulations, both by government institutions and the general public.

Enforcing laws against personal data protection violations presents significant challenges. At the regional level, limited legal instruments and insufficient law enforcement resources can impede efforts to effectively monitor and address such violations. To overcome these challenges, strategic measures are required to enhance the capacity of law enforcement personnel and improve coordination between central and regional governments.

To strengthen personal data protection in Gorontalo, the regional government should consider drafting a specific regional regulation (Peraturan Daerah) tailored to address personal data protection. Such a regulation can be adapted to local needs while reinforcing the implementation of the PDP Law at the regional level. Furthermore,

increasing digital literacy among both the community and government officials is crucial for fostering a culture of data security awareness. Education and training programs focusing on digital literacy must be promoted to enhance understanding of the importance of personal data protection.

In addition to these measures, improving technological infrastructure is a critical prerequisite for effective personal data protection. Regional governments must invest in developing robust technological systems, including the implementation of advanced encryption systems and comprehensive information security management frameworks. Collaboration with the private sector and academic institutions is also essential to strengthen technological capabilities and human resource expertise in managing personal data. This collaboration should extend to research and the development of innovative technological solutions to enhance data security and resilience against emerging threats.

3.2. Impact of Cybercrime on Victims: Protection and Recovery

Cybercrime has emerged as a significant threat in the digital era, causing profound psychological, financial, and social impacts on its victims.[15] This category of crime encompasses various violations, including identity theft, online fraud, hacking, and cyber harassment, all of which can result in substantial losses for individuals and organizations alike.[16] In response to the increasing prevalence of cybercriminal activity in Indonesia, the government has implemented stricter protective measures, including regulations aimed at safeguarding victims and addressing the losses they endure.

Victims of cybercrime often experience severe psychological trauma, particularly in cases involving identity theft or cyber harassment. For example, identity theft can leave victims feeling vulnerable and unsafe as their personal data is misused for unauthorized purposes. Similarly, cyber harassment, such as online bullying, can lead to significant emotional distress, including depression, anxiety, and, in extreme cases, suicidal ideation.

Financially, cybercrime frequently inflicts substantial losses on its victims. Online fraud, bank account hacking, and ransomware attacks can severely impact individuals' financial stability and, in many cases, disrupt the economic security of families and organizations. These financial repercussions often have a long-term domino effect, undermining broader economic stability.

On a social level, cybercrime can stigmatize victims and erode public trust. Victims whose sensitive personal information is leaked online or whose reputations are tarnished by smear campaigns often face social exclusion and reduced standing within their communities. These social consequences are particularly challenging to address and can

---

15 Joanna Curtis and Gavin Oxburgh, "Understanding Cybercrime In 'Real World' Policing and Law Enforcement," *The Police Journal: Theory, Practice and Principles* 96, no. 4 (2023): 333–42, https://doi.org/10.1177/0032258X221107584.

16 Gargi Sarkar and Sandeep K. Shukla, "Behavioral Analysis of Cybercrime: Paving the Way for Effective Policing Strategies," *Journal of Economic Criminology* 2, no. 100034 (2023), https://doi.org/10.1016/j.jeconc.2023.100034.

leave lasting scars on victims' lives. Efforts to combat cybercrime must address both preventive measures and comprehensive recovery strategies to mitigate these profound impacts on victims.

Law Number 27 of 2022 on Personal Data Protection (PDP Law) represents a significant legal effort to safeguard individuals from the impacts of cybercrime, particularly those related to the theft of personal data. This legislation imposes obligations on data controllers to ensure the protection of the personal data they manage, while also granting data subjects the right to seek compensation in cases of violations. Furthermore, the PDP Law prescribes criminal sanctions for individuals who commit offenses that breach personal data protection provisions.

However, relying solely on the PDP Law is insufficient to fully protect victims of cybercrime. The Indonesian government has also enacted Law Number 11 of 2008 on Information and Electronic Transactions (ITE Law), which has been amended through Law Number 19 of 2016. The ITE Law provides a legal foundation for prosecuting cybercrime offenders, specifying criminal sanctions for various cyber offenses, including defamation, online fraud, and unauthorized access to computer systems. This law equips victims of cybercrime with a legal basis to seek justice and restitution for their losses.

Additionally, Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions (PP 71/2019) mandates that electronic system operators protect personal data and secure their systems against cyber threats. This regulation provides guidelines for operators to implement robust security measures while also granting victims the right to access information and pursue recovery in the event of a data breach. Together, these legal instruments form a comprehensive framework aimed at addressing the multifaceted challenges posed by cybercrime and ensuring better protection for victims.

In Gorontalo, while there are no specific regional regulations addressing the protection of cybercrime victims, existing local regulations, particularly those concerning information technology governance and consumer protection, can be adapted to support these efforts. However, legal measures alone are insufficient without comprehensive recovery initiatives for victims. Such recovery must encompass multiple dimensions, including psychological, financial, and reputational aspects.

The government and relevant stakeholders must provide psychological support services, including counseling and therapy, to help victims cope with the trauma resulting from cybercrime. Financial recovery is equally critical and can be facilitated through mechanisms such as compensation or restitution for victims of online fraud. Furthermore, restoring the reputations of victims tarnished by cybercrime requires clear legal procedures to remove or take down harmful online content. This necessitates collaboration with digital platform providers and social media companies, which bear a responsibility to manage and eliminate unlawful content.

To enhance protection for victims, a holistic and multi-sectoral approach is imperative. This includes strengthening legal frameworks, improving digital literacy,

establishing comprehensive recovery services, and ensuring firm and effective law enforcement. Collaborative efforts involving the government, private sector, and civil society are essential to foster a secure and equitable digital ecosystem where individuals are safeguarded against cybercrime threats and have access to adequate remedies if victimized.

3.3. Implementation of Personal Data Protection Policies in Addressing Cybercrime

The implementation of personal data protection policies to combat cybercrime encompasses multiple interrelated dimensions that demand thorough attention. Holistically, these policies are not merely aimed at safeguarding individual information from unauthorized access but also represent a strategic initiative to foster trust within an increasingly complex digital ecosystem.[17] Personal data protection serves as a cornerstone for cultivating a sense of security in the use of information technology. When individuals feel confident that their data is adequately safeguarded, trust in digital systems grows, thereby facilitating the expansion of the digital economy and encouraging technological innovation.[18] However, challenges arising from technological, regulatory, and legal cultural factors act as significant barriers to effective data protection.

A critical aspect of this discussion is the practical implementation of existing regulations, such as Indonesia's Personal Data Protection (PDP) Law. While the PDP Law establishes a robust legal framework for safeguarding personal data, its effectiveness in practice remains a concern.

First, there exists a notable gap between the regulatory provisions and their practical application. Despite the PDP Law outlining comprehensive standards for data protection, its implementation often falls short due to inadequate technological infrastructure and limited human resource capacity to perform supervisory and law enforcement functions.

Second, the enforcement of laws against personal data violations requires significant improvement. Effective law enforcement is pivotal to the success of the PDP Law. However, enforcement efforts are frequently hindered by challenges such as insufficient coordination among law enforcement agencies, resource limitations, and the complex nature of cybercrime, which often involves transnational perpetrators. These challenges necessitate international cooperation and global legal harmonization to address transnational cybercrimes effectively.

Additionally, the regulatory framework must adapt to the dynamic nature of technological advancements. Cybercrime evolves continuously, introducing novel threats that may not be addressed by existing regulations. To mitigate these risks, it is imperative to conduct regular updates to existing laws and develop more specific derivative regulations tailored to emerging threats accompanying technological progress. Through these

---

17 Danil Erlangga Mahameru et al., "Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas Di Indonesia," *Jurnal Esensi Hukum* 5, no. 2 (2024): 115–31, https://doi.org/10.35586/jsh.v5i2.240.

18 Siti Yuniarti, "Perlindungan Hukum Data Pribadi Di Indonesia," *Jurnal Becoss: (Business Economic, Communication, and Social Sciences),* 1, no. 1 (2019): 147–54, https://doi.org/10.21512/becossjournal.v1i1.6030.

measures, the implementation of personal data protection policies can become a more effective mechanism for combating cybercrime, bolstering public trust, and promoting a secure digital environment.

The effectiveness of personal data protection is highly contingent upon the implementation of robust and comprehensive data security and cybersecurity measures. These elements are critical to any information system, as inadequate implementation and maintenance can significantly increase the risk of both financial and non-financial losses for organizations and other stakeholders. Properly securing data, both physically and digitally, ensures the achievement of the three fundamental principles of information security: confidentiality, integrity, and availability.

In Indonesia, the protection of personal data within the framework of data security and cybersecurity is explicitly governed by the Personal Data Protection Law. However, this protection is further reinforced through related regulations, including Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law), Government Regulation Number 71 of 2019 concerning the Operation of Electronic Systems and Transactions, and Regulation of the Minister of Communication and Information Technology Number 20 of 2016 regarding the Protection of Personal Data in Electronic Systems.

The Government Regulation on the Operation of Electronic Systems and Transactions mandates, particularly in Articles 18 and 69, that electronic system operators must regularly conduct cybersecurity audits. Moreover, Articles 65 to 72 establish the role of reliability certification bodies responsible for ensuring cybersecurity standards. These bodies issue reliability certificates that are vital for verifying that electronic system operators comply with Indonesian regulations and adhere to industry best practices.

Additionally, the Regulation of the Minister of Communication and Information Technology Number 20 of 2016 underscores the requirement for electronic system operators to establish internal regulations aimed at safeguarding personal data. These internal privacy policies are designed to prevent failures in protecting managed data. Typically, electronic system operators that act as personal data controllers must develop both internal privacy policies and external privacy policies (commonly referred to as privacy notices). These policies play a crucial role in ensuring the integrity of data protection frameworks and maintaining trust in digital systems. By aligning operational practices with these legal requirements and industry standards, organizations can enhance their resilience against cybersecurity threats and foster a safer digital environment for personal data management.

In personal data processing, the Regulation of the Minister of Communication and Information Technology mandates that electronic system organizers provide transparent information and obtain consent from data owners in alignment with the intended purpose of data processing. This regulation establishes a clear legal foundation, particularly during data collection, ensuring that all subsequent processing or analysis adheres strictly to the consent initially granted.

When transmitting personal data, several critical factors must be considered, including the method of transfer, the specific purpose, the accuracy of the data, and the data owner's consent. Data must undergo verification to ensure accuracy and compliance with the agreed terms of consent. Furthermore, cross-border data exchange must be governed by stringent protocols to maintain data integrity and security. Data storage protocols emphasize encryption and classification based on established data management or privacy policies.

For data destruction, electronic system organizers are required to implement clear retention schedules, procedures, and accountability measures to ensure periodic deletion in line with applicable policies. These measures aim to minimize risks associated with unnecessary data retention and safeguard personal data throughout its lifecycle.

From the victim's perspective, personal data protection extends beyond prevention to encompass recovery. When personal data protection policies are effectively implemented, victims of cybercrime have a structured avenue to seek legal and psychological recovery. However, gaps in policy implementation often exacerbate the plight of victims, leading to increased financial and emotional harm.

To address these shortcomings, the legal framework must incorporate robust redress mechanisms for cybercrime victims. This necessitates a more proactive approach from the government and law enforcement agencies in monitoring and enforcing regulations. Additionally, digital service providers bear the responsibility of safeguarding user data by employing advanced security technologies that adhere to international standards.

Collaboration among stakeholders is vital in tackling this challenge. Governments, law enforcement, digital service providers, and communities must work collectively to foster a secure and trustworthy digital environment. Public education campaigns are also crucial, raising awareness about the importance of personal data protection and equipping individuals with strategies to safeguard themselves against cybercrime threats. Together, these efforts can create a resilient digital ecosystem that prioritizes both prevention and recovery in the face of cybercrime.

CONCLUSION

Based on the research findings, personal data protection is not merely an issue of information security but is deeply intertwined with human rights, particularly the right to privacy. While regulations such as Law Number 27 of 2022 on Personal Data Protection provide a legal framework, their implementation faces numerous challenges. One significant issue is the low level of public awareness regarding the importance of personal data protection. Additionally, inadequate technological infrastructure and limited law enforcement capabilities present substantial obstacles. Current regulations often fall short of addressing the increasing complexity and evolving nature of cybercrime.

Cybercrime has severe impacts on victims, ranging from financial losses to psychological and social trauma. Many victims feel powerless, as the existing legal system does not always offer sufficient protection or recovery mechanisms. The transnational

nature of cybercrime exacerbates the difficulty of enforcement, requiring stronger international cooperation and a comprehensive approach. To address these challenges, personal data protection policies must be continuously updated, incorporating legal, technological, and public education components. Improving public digital literacy is particularly crucial to better equip individuals to safeguard their personal data.

In the context of Gorontalo Province, strategic measures are essential to address these challenges effectively. Public digital literacy should be prioritized through ongoing education campaigns, enabling individuals to recognize cyber threats and adopt preventive measures. Additionally, the government must urgently invest in robust technological infrastructure, including advanced security systems featuring data encryption and threat detection capabilities. At the local level, the development of specific regional regulations (Peraturan Daerah or Perda) could bolster the enforcement of national policies, ensuring that both government institutions and the private sector adhere to data protection standards.

Collaborative efforts among stakeholders—government, private sector, law enforcement, and civil society—are indispensable to creating a secure digital environment. By integrating educational initiatives, technological advancements, and regulatory frameworks, Gorontalo can strengthen its resilience against cybercrime and enhance the protection of personal data for its citizens.

REFERENCES

Journals

Bangsawan, Gema. "Kebijakan Akselerasi Transformasi Digital Di Indonesia: Peluang Dan Tantangan Untuk Pengembangan Ekonomi Kreatif." *Jurnal Studi Kebijakan Publik* 2, no. 1 (2023): 27–40. https://doi.org/10.21787/jskp.2.2023.27-40.

Butarbutar, Russel. "Kejahatan Siber Terhadap Individu: Jenis , Analisis , Dan Perkembangannya." *Technology and Economiacs Law Journal* 2, no. 2 (2023): 297–316. https://doi.org/10.21143/TELJ.vol2.no2.1043.

Curtis, Joanna, and Gavin Oxburgh. "Understanding Cybercrime In 'Real World' Policing and Law Enforcement." *The Police Journal: Theory, Practice and Principles* 96, no. 4 (2023): 333–42. https://doi.org/10.1177/0032258X221107584.

Disemadi, Hari Sutra, Lu Sudirman, Junimart Girsang, and Meida Aninda. "Perlindungan Data Pribadi Di Era Digital: Mengapa Kita Perlu Peduli?" *Sang Sewagati Journal* 1, no. 2 (2023): 67–90. https://doi.org/10.37253/sasenal.v1i2.8579.

Firdaus, Indriana. "Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan." *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia* 4, no. 2 (2022): 23–31. https://doi.org/10.52005/rechten.v4i2.98.

Galih Hariyono, Akbar, and Frans Simangunsong. "Perlindungan Hukum Korban Pencurian Data Pribadi (Phishing Cybercrime) Dalam Perspektif Kriminologi."

Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance 3, no. 1 (2023): 1–12. https://doi.org/10.53363/bureau.v3i1.191.

Jupri, Jupri, Arhjayati Rahim, Rusmulyadi Rusmulyadi, Vicky Ibrahim, and Umar P. "A Model of Legal Culture for Prevention of Money Politics Through Social Media Strategies for Facing Simultaneous Elections in 2024 Gorontalo Province." *Jurnal Hukum Volkgeist* 8, no. 1 (2023): 123–32. https://www.jurnal-umbuton.ac.id/index.php/Volkgeist/article/view/4356.

Mahameru, Danil Erlangga, Aisyah Nurhalizah, Haikal Badjeber, Ahmad Wildan, and Haikal Rahmadia. "Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas Di Indonesia." *Jurnal Esensi Hukum* 5, no. 2 (2024): 115–31. https://doi.org/10.35586/jsh.v5i2.240.

Sarkar, Gargi, and Sandeep K. Shukla. "Behavioral Analysis of Cybercrime: Paving the Way for Effective Policing Strategies." *Journal of Economic Criminology* 2, no. 100034 (2023). https://doi.org/10.1016/j.jeconc.2023.100034.

Sihombing, L. Alfies, and Yeni Nuraeni. "Norms and Ethics in Criminal Justice: Assessing Contemporary Legal Policy." *Jurnal Info Sains: Informatika Dan Sains* 13, no. 3 (2023): 1088–1099. https://ejournal.seaninstitute.or.id/index.php/InfoSains/article/view/3693.

Widianingrum, Afifah Rizqy. "Analisis Implementasi Kebijakan Hukum Terhadap Penanganan Kejahatan Siber Di Era Digital." *Journal Iuris Scientia* 2, no. 2 (2024): 90–102. https://doi.org/10.62263/jis.v2i2.40.

Yunani, Farhan A, and Andi Aina Ilmih. "Kajian Yuridis Kejahatan Lintas Negara Berkaitan Dengan Perlindungan Data Pribadi." *Media Hukum Indonesia* 2, no. 3 (2024): 586–92. https://ojs.daarulhuda.or.id/index.php/MHI/article/view/660.

Yuniarti, Siti. "Perlindungan Hukum Data Pribadi Di Indonesia." *Jurnal Becoss: (Business Economic, Communication, and Social Sciences),* 1, no. 1 (2019): 147–54. https://doi.org/10.21512/becossjournal.v1i1.6030.

Thesis

Kholiviya, Hasna. "Perlindungan Hukum Terhadap Korban Pencurian Data Pribadi Dalam Kasus Tindak Pidana Mayantara (Cyber Crime)." Universitas Islam Sultan Agung Semarang, 2021. https://repository.unissula.ac.id/24642/.

Books

Fajar, M, and A Yulianto. *Dualisme Penelitian Hukum Dan Empiris*. Jakarta: Pustaka Pelajar, 2010.

Soekanto, Soerjono, and Sri Mamudji. *Penelitian Hukum Normatif : Suatu Tujuan Singkat*. Jakarta: PT.Raja Grafindo Persada, 2003.

Regulations

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

Web Pages

Nawu, Apris. "Data Kependudukan Warga Gorontalo Bocor Di Internet, Pelaku Petugas Puskesmas." Detiksulsel, 2023. https://www.detik.com/sulsel/berita/d-6921091/data-kependudukan-warga-gorontalo-bocor-di-internet-pelaku-petugas-puskesmas.