

LEGAL PROTECTION FOR CYBERCRIME VICTIMS REGARDING PERSONAL DATA HANDLING AT THE BALI REGIONAL POLICE

Kadek Wahyudi Putra Pranata¹
Universitas Mahendradatta

Ni Ketut Wiratny²
Universitas Mahendradatta

Sobandi³
Universitas Mahendradatta

Correspondence : Kadek Wahyudi Putra Pranata (kadekwahyudiputrapranata95@gmail.com)

Abstract

The rapid development of information technology has transformed various aspects of human activities into digital platforms. Alongside these advancements, cybercrime has significantly increased, particularly crimes involving the misuse of personal data. Such crimes result not only in financial losses but also in violations of privacy, security, and legal certainty for victims. Consequently, effective legal protection is required through the active role of law enforcement agencies, especially the Bali Regional Police, in handling cybercrime cases involving personal data. This research employs normative legal research supported by empirical research. The study applies statutory, conceptual, and factual approaches. Data were collected through library research and interviews with investigators of the Cyber Crime Directorate of the Bali Regional Police. The collected data were analyzed qualitatively using descriptive methods. The results indicate that legal protection for victims of cybercrime at the Bali Regional Police is implemented through preventive measures such as digital literacy education, public awareness regarding personal data protection, improvement of electronic security systems, and institutional cooperation. Repressive measures include receiving public reports, conducting investigations, examining digital evidence, and enforcing criminal law under the Electronic Information and Transactions Law and the Personal Data Protection Law. However, several obstacles remain, including limited cyber forensic experts, inadequate digital forensic facilities, the complexity of electronic evidence, and low public awareness regarding personal data protection. Therefore, strengthening investigators' capacity, improving digital forensic infrastructure, and enhancing inter-agency cooperation are necessary to achieve more effective legal protection for cybercrime victims.

Keywords: Legal Protection, Cybercrime Victims, Personal Data, Law Enforcement.

INTRODUCTION

Advancements in information technology have fundamentally transformed societal patterns of life. The internet has become a primary medium for economic activities, education, e-commerce, public services, and daily communication. While this digitalization drives efficiency, it also creates opportunities for new forms of crime that utilize information technology as either the medium or the target of criminal acts. Cybercrime is a form of criminality that evolves rapidly alongside technological progress. It differs from conventional crime in that it is perpetrated via electronic systems, is transnational in nature, exploits perpetrator anonymity, and relies on constantly evolving technology. Consequently, identifying

perpetrators and establishing proof of the offense are far more complex than in conventional criminal cases.

One of the most damaging forms of cybercrime is the misuse of personal data. Personal data currently holds significant economic value, making it a target for various crimes such as identity theft, phishing, hacking, illegal interception, banking account misuse, and digital-based fraud. Such misuse not only causes financial loss but also threatens the privacy rights, security, and even the reputations of victims. Indonesia has addressed these developments through various regulations, notably Law Number 27 of 2022 concerning Personal Data Protection and Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. The enactment of these regulations demonstrates the state's commitment to ensuring legal certainty for individuals who fall victim to personal data misuse in the digital realm.

In the practice of law enforcement, the Indonesian National Police is authorized to conduct preliminary inquiries and formal investigations into cybercrimes, as stipulated by Law Number 2 of 2002 concerning the Indonesian National Police. In Bali, the growth of digital economic activities and the tourism sector has heightened the risk of personal data misuse. Data from the Bali Regional Police regarding case handling indicates a significant rise in cases involving the misuse of personal data, thereby necessitating a more comprehensive legal protection strategy. Legal protection for victims is not achieved solely through the punishment of perpetrators; it also encompasses the protection of the victim's identity, restitution for losses, the provision of updates on case progress, and security guarantees throughout the legal proceedings. This approach aligns with modern victimology concepts, which position the victim as a subject deserving of attention within the criminal justice system.

Given these circumstances, this study addresses two research questions: how legal protection for cybercrime victims is implemented regarding personal data handling at the Bali Regional Police, and what obstacles are encountered in the implementation of such protection.

METHOD

This study is a normative legal study supported by empirical legal research. The normative approach is employed to examine statutory provisions regarding personal data protection, victim protection, and law enforcement against cybercrimes, while the empirical approach is used to gather data on the implementation of legal protection for victims at the Bali Regional Police through interviews with law enforcement officials. The research methodology incorporates the statute approach, the conceptual approach, and the fact approach. Legal materials consist of primary sources (legislation), secondary sources (books, scholarly journals,

and research findings), and tertiary sources (legal dictionaries and encyclopedias). All legal materials are analyzed qualitatively using a descriptive-analytical method and deductive reasoning to arrive at systematic conclusions.

RESULTS AND DISCUSSION

Legal Protection for Cybercrime Victims Regarding Personal Data Handling at the Bali Regional Police

Legal protection for victims of cybercrime constitutes a form of state responsibility to ensure the fulfillment of citizens' constitutional rights, as mandated by Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which guarantees the protection of personal safety, family, honor, dignity, and a sense of security for every citizen. In the context of information technology advancements, this form of protection has expanded to include the protection of personal data as part of the right to privacy. This right is currently comprehensively regulated under Law Number 27 of 2022 concerning Personal Data Protection, which obliges the state to provide protection against any unlawful processing of personal data.

The Bali Regional Police (Polda Bali), as part of the Indonesian National Police, is authorized to conduct inquiries and investigations into cybercrimes, as stipulated in Law Number 2 of 2002 concerning the Indonesian National Police and Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. Research findings indicate that legal protection for victims is implemented through two primary approaches: preventive legal protection and repressive legal protection.

1. Preventive Legal Protection

Preventive legal protection aims to prevent legal violations before they result in victims. Philipus M. Hadjon explains that preventive protection is a form of protection provided through the establishment of legal norms, ensuring the public has certainty regarding their rights and obligations before disputes arise. In addressing cybercrime, preventive protection is crucial, given that the characteristics of cybercrime evolve more rapidly than regulations or the public's capacity to understand digital security. Research shows that the Bali Regional Police actively conducts various educational activities for the public regarding the importance of safeguarding personal data confidentiality. This education is carried out through legal outreach and awareness campaigns targeting educational institutions, government agencies, and community groups, as well as by utilizing the Bali Regional Police's official social media channels to disseminate information on emerging cybercrime methods. These efforts aim to enhance public

digital literacy, enabling people to recognize various forms of online fraud, phishing, social engineering, identity theft, and the misuse of personal data.

In addition to public outreach activities, the Bali Regional Police (Polda Bali) also establishes coordination with ministries, government agencies, electronic system operators, banking institutions, and telecommunications service providers to strengthen electronic data security systems. This collaboration aims to accelerate the identification of perpetrators' accounts, the tracking of electronic transactions, the blocking of bank accounts, and the recovery of systems affected by cyberattacks. Preventive protection is also realized by enhancing the capacity of law enforcement officers through education and training in digital forensics, cyber investigations, and the handling of electronic evidence. These measures are crucial given the highly dynamic nature of information technology developments; law enforcement officers must continuously upgrade their competencies to keep pace with evolving cybercrime **modi operandi**. According to Philipus M. Hadjon's theory of legal protection, these preventive measures represent an implementation of the rule of law that focuses not only on punishing perpetrators but also on preventing victimization through the strengthening of regulations, education, and oversight.

Repressive Legal Protection

Repressive legal protection is provided after a criminal offense has occurred. This protection aims to restore victims' rights while enforcing the law against perpetrators. In cybercrime cases, repressive protection involves greater complexity than in conventional crimes because much of the evidence consists of electronic information requiring digital forensic processes. Research findings indicate that the repressive protection mechanism at the Bali Regional Police begins with the receipt of public reports via the Integrated Police Service Center (SPKT). Once a report is received, investigators from the Cyber Investigation Directorate conduct a preliminary inquiry to determine whether the elements of a criminal offense exist, as stipulated in the Law on Electronic Information and Transactions and the Law on Personal Data Protection. Subsequently, a formal investigation is conducted, involving the questioning of witnesses, victims, and experts; the seizure of electronic evidence; digital forensic analysis; and the tracing of the perpetrator's identity.

Throughout this process, victims receive various forms of legal protection, including:

1. the right to report a criminal offense easily and without discrimination;
 2. the right to obtain information regarding the progress of the case;
 3. the right to confidentiality of identity, if necessary;
 4. the right to receive assistance during the investigation process;
-

5. the right to receive protection under Law Number 31 of 2014 concerning the Protection of Witnesses and Victims;
6. the right to claim restitution in accordance with statutory provisions, provided the requirements are met.

The implementation of such protection demonstrates that the law enforcement system is no longer solely offender-oriented but has begun to accommodate the interests of victims (victim-oriented). This approach aligns with the evolution of modern victimology, which positions the victim as a subject entitled to protection, restitution, and legal certainty. According to Arif Gosita, victims of criminal acts require comprehensive protection because the harm they suffer is not merely material but also psychological and social, potentially affecting their long-term quality of life. This is particularly relevant for victims of personal data misuse, who often face economic losses, the loss of digital identity, and psychological distress resulting from the dissemination of personal information without consent.

Analysis of the Implementation of Legal Protection

When analyzed using Soerjono Soekanto's law enforcement theory, the implementation of legal protection for cybercrime victims at the Bali Regional Police (Polda Bali) is influenced by five key factors: the law itself, law enforcement officers, facilities and infrastructure, the community, and legal culture. Regarding regulations, Indonesia possesses a relatively adequate legal framework comprising the Personal Data Protection Law, the Electronic Information and Transactions Law, the Witness and Victim Protection Law, and the Criminal Procedure Code. These regulations provide the legal basis for investigators to handle criminal cases involving the misuse of personal data.

From an institutional perspective, the Bali Regional Police has demonstrated a strong commitment by establishing specialized cybercrime units, enhancing investigator capabilities, and fostering inter-agency coordination. However, the effectiveness of legal protection remains constrained by limited human resources and the fact that technological advancements outpace the capacity-building of law enforcement officers. Furthermore, the public's level of digital literacy remains a major challenge; many victims only report crimes after suffering significant losses, and some individuals still provide personal data to unauthorized parties without prior verification. This situation demonstrates that legal protection for victims cannot rely solely on a repressive approach; rather, it must be balanced by fostering a culture of legal awareness among the public through continuous digital education.

Thus, legal protection for cybercrime victims at the Bali Regional Police has been implemented in accordance with the prevailing normative framework. However, its

effectiveness still requires strengthening through human resource capacity building, the modernization of digital forensic technology, enhanced inter-agency coordination, and the improvement of public digital literacy, so that the objectives of legal protection—namely justice, legal certainty, and utility—can be optimally realized.

Challenges Faced by the Bali Regional Police in Providing Legal Protection to Cybercrime Victims Regarding the Handling of Personal Data

Legal protection for cybercrime victims depends not only on the existence of adequate legislation but also on the effectiveness of law enforcement officials in carrying out their duties. Although Indonesia possesses various regulations—such as Law Number 27 of 2022 concerning Personal Data Protection, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, and Law Number 31 of 2014 concerning the Protection of Witnesses and Victims—the implementation of legal protection for cybercrime victims still faces numerous obstacles. Research conducted at the Bali Regional Police (Polda Bali) indicates that these obstacles stem from issues regarding human resources, facilities and infrastructure, evidentiary processes, regulations, and societal factors.

Limited Human Resources in the Cyber Sector

A primary obstacle is the limited number of investigators possessing specialized competence in cybercrime and digital forensics. Cybercrime is an offense requiring high-level technical skills, as the evidentiary process involves analyzing electronic devices, computer networks, cloud computing systems, and digital transactions, as well as tracing electronic identities. Rapid technological advancements necessitate that investigators continuously update their skills through ongoing education and training. However, not all investigators have the opportunity to obtain certification or specialized training in digital investigation. Consequently, the investigation process for certain cases takes longer than that for conventional crimes. According to Soerjono Soekanto, the quality of law enforcement officials is a key factor determining the success of law enforcement. The professionalism of these officials influences the state's ability to provide legal certainty and protection to the public.

Limitations of Digital Forensics Facilities

Another challenge lies in the limitations of digital forensics facilities and infrastructure. In cybercrime investigations, electronic evidence requires identification processes using specialized software and hardware. Examining mobile phones, computers, servers, digital storage media, or electronic accounts necessitates an adequate digital forensics laboratory. Not all cases can be resolved quickly, as certain examinations must be conducted in collaboration

with higher-level digital forensics laboratories. This situation prolongs the investigation process, particularly when evidence involves encryption, cloud storage, or servers located outside Indonesian territory. According to Edmon Makarim, the evolution of information technology requires law enforcement agencies to possess modern digital infrastructure; without technological support, the effectiveness of cybercrime law enforcement faces significant obstacles.

Complexity of Establishing Electronic Evidence

Cybercrimes differ in nature from ordinary criminal offenses because the primary forms of evidence are electronic information and electronic documents. Digital evidence can easily be altered, deleted, moved, or even concealed by perpetrators using specific technologies. Furthermore, perpetrators often employ false identities, virtual private networks (VPNs), overseas servers, anonymous accounts, and even cryptocurrency, thereby adding layers of complexity to the identification process.

In practice at the Bali Regional Police (Polda Bali), investigators must coordinate with various entities—such as electronic system providers, banks, telecommunications operators, and relevant ministries—to obtain data supporting the investigation. This process is time-consuming, as it must adhere to applicable legal procedures. Peter Mahmud Marzuki states that the establishment of proof in modern law no longer relies solely on conventional evidence; rather, it evolves alongside advancements in information technology, necessitating legal interpretations that adapt to societal developments.

Low Public Legal Awareness

Public-related factors also constitute a significant obstacle. Research indicates that many members of the public still do not grasp the importance of safeguarding personal data. Some individuals readily disclose identification numbers, OTP codes, PINs, passwords, or bank account details to unknown parties. Furthermore, victims often delay reporting crimes due to feelings of shame, fear of being blamed, or the belief that their losses are irrecoverable. Consequently, the opportunity for investigators to trace electronic transactions or identify perpetrators diminishes. From the perspective of Soerjono Soekanto's theory of legal effectiveness, low public legal awareness is a key factor preventing law enforcement from functioning optimally.

The Transnational Nature of Cybercrime

Unlike conventional crimes, cybercrime is frequently committed across regional or even national borders (transnational organized crime). Perpetrators can commit crimes from another country without ever entering Indonesian territory. This situation necessitates law

enforcement cooperation through mechanisms such as Mutual Legal Assistance (MLA), international police cooperation (INTERPOL), and coordination with international digital service providers. If the perpetrator is located outside Indonesian jurisdiction, the investigation process takes significantly longer, as it must adhere to international legal mechanisms.

Analysis of Obstacles Based on Law Enforcement Theory

When analyzed using Soerjono Soekanto's law enforcement theory, these various obstacles indicate that the effectiveness of legal protection is influenced by five key factors.

1. First, the legal framework has seen positive developments with the enactment of the Personal Data Protection Law and amendments to the ITE Law. However, the evolution of cybercrime **modus operandi** far outpaces regulatory developments, necessitating continuous legal updates.
2. Second, regarding law enforcement personnel, there is a need to enhance human resource capacity through education and training in digital forensics.
3. Third, the infrastructure factor requires significant investment in digital forensics laboratories, electronic analysis tools, and cybersecurity systems.
4. Fourth, regarding the public, low digital literacy levels persist, making individuals easy targets for perpetrators.
5. Fifth, the legal culture factor indicates that the public has not yet fully integrated personal data security into their daily legal culture.

Therefore, enhancing the effectiveness of legal protection for cybercrime victims cannot be achieved solely through the creation of new regulations; it must also be accompanied by improvements in the quality of law enforcement personnel, the modernization of investigative technology, the strengthening of cross-sector cooperation, and sustained efforts to improve public digital literacy.

CONCLUSION

Based on the research findings, it can be concluded that:

1. Legal protection for cybercrime victims regarding personal data handling by the Bali Regional Police (Polda Bali) has been implemented through two forms of protection: preventive and repressive legal protection. Preventive protection is carried out through digital literacy education, raising awareness about personal data security, increasing public awareness, and collaborating with various agencies to strengthen information security systems. Meanwhile, repressive protection is realized through the acceptance of victim reports, preliminary inquiries, formal investigations, the examination of

electronic evidence, digital forensics, and law enforcement based on the provisions of the Electronic Information and Transactions Law, the Personal Data Protection Law, and the Witness and Victim Protection Law. The implementation of such protection demonstrates that the Bali Regional Police has endeavored to provide legal certainty as well as protection for the rights of cybercrime victims.

2. The implementation of legal protection still faces various obstacles, including a shortage of personnel competent in digital forensics, limited investigative facilities and infrastructure, the complexity of establishing electronic evidence, low public awareness regarding personal data security, and the transnational nature of cybercrime. Therefore, enhancing investigator capacity, modernizing digital forensic facilities, strengthening inter-agency coordination, updating regulations to adapt to technological advancements, and improving public digital literacy constitute strategic steps toward achieving more effective legal protection for cybercrime victims.

Recommendation

1. Polda Bali perlu meningkatkan kompetensi penyidik melalui pendidikan dan sertifikasi di bidang investigasi siber dan digital forensik secara berkelanjutan.
2. Masyarakat perlu diberikan edukasi secara berkelanjutan mengenai perlindungan data pribadi, keamanan transaksi elektronik, dan pentingnya pelaporan dini apabila menjadi korban kejahatan siber.

REFERENCES

- Arief, Barda Nawawi. 2010. **Cyber Crime (Tindak Pidana Mayantara)**. RajaGrafindo Persada, Jakarta.
- Criminal Procedure Code (KUHP), Law Number 8 of 1981 concerning Criminal Procedure Law (State Gazette of the Republic of Indonesia of 1981 Number 76, Supplement to the State Gazette of the Republic of Indonesia Number 3209).
- Erman Rajagukguk. 2005. "The Role of Law in Economic Development." *Journal of Business Law*, Vol. 24, No. 1.
- Gosita, Arif. 2003. **Issues Regarding Crime Victims**. Akademika Pressindo, Jakarta.
- Hadjon, Philipus M. 2007. **Legal Protection for the People in Indonesia**. Bina Ilmu, Surabaya.
- Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (State Gazette of the Republic of

Indonesia of 2024 Number 1, Supplement to the State Gazette of the Republic of Indonesia Number 6905).

Law Number 2 of 2002 concerning the Indonesian National Police (State Gazette of the Republic of Indonesia of 2002 Number 2, Supplement to the State Gazette of the Republic of Indonesia Number 4168).

Law Number 27 of 2022 concerning Personal Data Protection (State Gazette of the Republic of Indonesia of 2022 Number 196, Supplement to the State Gazette of the Republic of Indonesia Number 6820).

Law Number 31 of 2014 concerning Amendment to Law Number 13 of 2006 concerning Witness and Victim Protection (State Gazette of the Republic of Indonesia of 2014 Number 293, Supplement to the State Gazette of the Republic of Indonesia Number 5602).

Makarim, Edmon. 2020. **Introduction to Telematics Law: A Compilation of Studies**. PT RajaGrafindo Persada, Depok.

Marzuki, Peter Mahmud. 2016. **Legal Research**. Kencana, Jakarta.

Maskun. 2013. **Cyber Crime: An Introduction**. Kencana, Jakarta.

Rosadi, Sinta Dewi. 2021. **Personal Data Protection in Indonesia**. PT Refika Aditama, Bandung.

Soekanto, Soerjono. 2008. **Factors Influencing Law Enforcement**. RajaGrafindo Persada, Jakarta.

The 1945 Constitution of the Republic of Indonesia.