E-ISSN: 3032-0135
Vol. 4, No.1, July - December (2026), pp. 371 - 377

Law Enforcement Against Personal Data Hacking Offenses by the Cyber Investigation Directorate of the Bali Regional Police

Putu Pradnyamita Setianingtyas[1]
Universitas Mahendradatta

Sobandi[2]
Universitas Mahendradatta

I Made Mulyawan Subawa[3]
Universitas Mahendradatta

Correspondence : Putu Pradnyamita Setianingtyas (pradnyamita@gmail.com)

Abstract

The rapid development of information technology has not only transformed people's lifestyles but has also triggered the evolution of conventional crime into modern forms of cybercrime, one of which is the crime of hacking personal data. This study aims to analyze the effectiveness of law enforcement against the crime of hacking personal data by the Bali Regional Police Cyber Investigation Directorate and identify the obstacles faced in the enforcement process. The research method used is empirical juridical with a statutory, conceptual, and case approach, where data collection was carried out through literature studies and in-depth interviews with internal parties of the Bali Regional Police Cyber Investigation Directorate. The results of the study indicate that law enforcement against the crime of hacking personal data from 2024 to May 2026 in the jurisdiction of the Bali Regional Police has been implemented in an integrated manner through a repressive, pro-justicia and preventive approach, which is reflected in the decreasing trend in the number of reports from 18 reports (2024), 9 reports (2025), to 2 reports (May 2026). The majority of cases are resolved through the Investigation Termination Order (SP3). However, the investigation process still faces complex obstacles due to the cross-border nature of the crime, the anonymity of perpetrators who utilize VPN and proxy technology, the placement of servers abroad, and the low level of legal awareness among the public regarding protecting their personal data. Continuous strengthening of the legal structure, substance, and culture, along with cross-sectoral and international cooperation, are key determinants for optimizing legal protection for the public's personal data.

Keywords: Law Enforcement, Personal Data Hacking, Cybercrime, Legal System, Bali Regional Police.

INTRODUCTION

The rapid advancement of information and communication technology has transformed various aspects of global life, driving a shift toward boundless digitalization. While this phenomenon has brought significant efficiency and progress to many areas of life, the evolving digital landscape has simultaneously spurred a transformation in the nature of crime - shifting from conventional methods to modern forms, most notably through cybercrime. Hacking, which originally served the constructive purpose of testing system security, has morphed into an illicit tool for breaching systems to exploit personal data. Given that personal data currently holds immense economic value, it has become a prime target for identity theft - whether for illicit gain or as a commodity on the black market.

Personal data protection is essentially an embodiment of the right to privacy - recognized as a fundamental human right in both international instruments, such as Article 12 of the Universal

E-ISSN: 3032-0135
Vol. 4, No.1, July - December (2026), pp. 371 - 377

Declaration of Human Rights (UDHR), and domestic instruments, specifically Article 28G paragraph (1) of the 1945 Constitution. The Indonesian government has specifically strengthened this regulatory framework through Law Number 27 of 2022 concerning Personal Data Protection, aligned with Article 26 of Law Number 1 of 2024 (regarding the Second Amendment to the ITE Law) and the Regulation of the Minister of Communication and Informatics Number 20 of 2016. These regulations explicitly guarantee the constitutional rights of data subjects, grant the right to object, and enable data owners to file lawsuits seeking redress for damages resulting from the misuse of electronic information.

However, at an empirical level, there remains a significant gap between the law as envisioned (das Sollen) and the reality of law enforcement on the ground (*das Sein*). The complex, cross-border nature of cybercrime, compounded by limitations in both the number and technical capacity of law enforcement personnel, often poses serious obstacles to the processes of gathering evidence and tracking down perpetrators. The phenomenon of cybercrime represents the dark side of technological advancement, bringing widespread negative impacts across all areas of life. One of its primary manifestations is hacking—the act of unlawfully breaching another party's computer network to extract specific data, gain unauthorized access to digital devices, or even damage digital systems. Although the practice of tinkering with these systems initially offered benefits to technology experts by helping them discover software vulnerabilities (bugs), its misuse in the modern era has proven highly detrimental to society.

To provide a concrete example, data from the Bali Regional Police's Cyber Investigation Directorate covering the period from 2024 through May 2026 records 29 police reports regarding personal data hacking. Although statistics indicate a downward trend in cases, the situation on the ground reveals the high complexity of the investigations. Real-world cases—such as the hacking of social media accounts belonging to individuals or business entities within the jurisdiction of the Bali Regional Police—often result in the misuse of those accounts for online gambling content or financial fraud (e.g., fake giveaways). Investigations are frequently hindered by technical authentication issues, ultimately leading to the withdrawal of reports or the issuance of an Order to Terminate Investigation (SP3). This gap underscores the necessity for a legal framework that not only ensures the smooth progress of national development and safeguards its outcomes but also effectively protects the rights of the parties involved and takes firm action against cybercriminals. Therefore, integrated law enforcement reform is required-strengthening the structural, substantive, and cultural aspects of the law-to ensure legal certainty and the effective protection of the public's personal data in the digital era.

1.1 Problem Statement

Based on the background discussion above, the problem formulation can be defined as follows:

E-ISSN: 3032-0135
Vol. 4, No.1, July - December (2026), pp. 371 - 377

first, to examine law enforcement regarding the criminal offense of personal data hacking by the Cyber Investigation Directorate of the Bali Regional Police; and second, to identify the obstacles encountered in such law enforcement efforts.

1.2 Purpose of the Writing

This study aims to examine and understand the law enforcement actions taken by the Cyber Investigation Directorate of the Bali Regional Police regarding the crime of personal data hacking, while identifying potential obstacles encountered during the process.

1.3 Research Methods

This study employs an empirical-juridical research approach, examining and analyzing the operation of law within society (law in action) through primary data. Empirical research constitutes field research—that is, research conducted systematically and methodologically to gather necessary data directly from the field or research site. The approach employed consists of three types: the statutory approach, the conceptual approach, and the case approach. Data collection was conducted through a literature review of similar studies and interviews with relevant parties. The gathered data was then processed and analyzed using qualitative methods and systematically compiled to provide an overview of the issue under study.

Results and Discussion

2.1 Case Detection and Case Resolution

Hacking has become a significant concern amidst today's technological advancements. The public has experienced numerous incidents in recent years. According to data from the Bali Regional Police's Cyber Investigation Directorate, the cases of personal data hacking recorded between 2024 and 2026 are as follows:

Table 1.1

Personal Data Hacking Cases, 2024–2026

NO	YEAR	POLICE REPORT	CASE RESOLUTION	
1	2024 (January–December)	18	SP 3 RJ LIDIK	: 16 : 1 : 1
2	2025 (January–December)	9	SP 3	: 9
3	2026 (January-May)	2	LIDIK	: 2
TOTAL NUMBER		**29**	**29**	

Data from the Cyber Crime Investigation Directorate (Ditressiber) of the Bali Regional Police

E-ISSN: 3032-0135
Vol. 4, No.1, July - December (2026), pp. 371 - 377

indicates a downward trend in police reports regarding personal data hacking offenses between 2024 and May 2026. A total of 29 reports were recorded, comprising 18 in 2024, 9 in 2025, and 2 up to May 2026. Regarding case handling, the resolution dynamics show that not all cases proceeded to trial; in 2024, 16 cases were terminated (via SP3), one was resolved through restorative justice, and one remained under investigation, whereas all cases from 2025 were terminated (SP3), and the two reports from 2026 are still under investigation. The high number of cases terminated via *SP3* (Order to Terminate Investigation) does not substantially reflect a failure in law enforcement; rather, it represents an adherence to the principle of legal certainty in instances where there is insufficient evidence or the event is proven not to constitute a criminal offense. Indeed, the overall downward trend in cases indicates the success of combining accountable law enforcement with an optimized preventive approach.

When analyzed through the lens of Lawrence M. Friedman's legal system theory, the effectiveness of cyber law enforcement within the Bali Regional Police jurisdiction is shaped by the integration of three interconnected elements. First, regarding legal structure, the Cyber Crime Investigation Directorate (Ditressiber) of the Bali Regional Police has established a specialized unit competent in digital forensics—mandated by Indonesian National Police Regulation No. 3 of 2024—and bolstered by cross-sector collaboration to secure electronic evidence. Second, concerning legal substance, investigators operate upon a progressive normative foundation provided by Law No. 1 of 2024 (ITE Law), Law No. 27 of 2022 (PDP Law), the Criminal Procedure Code (KUHAP), and Police Regulation No. 8 of 2021, which accommodates restorative justice approaches. Third, regarding legal culture, the Directorate actively mitigates digital vulnerabilities through cyber patrols, literacy initiatives, and public education aimed at boosting community participation and legal awareness. The synergy of these three components demonstrates that law enforcement regarding personal data hacking by the Bali Regional Police has shifted from a purely punitive approach toward a more holistic system focused on protection and social restoration.

2.2 Obstacles in Law Enforcement Against Personal Data Hacking Offenses by the Cyber Investigation Directorate of the Bali Regional Police

The rapid acceleration of global information and communication technology has blurred conventional boundaries and transformed social, economic, and cultural landscapes—as well as the realm of law enforcement—through the emergence of cybercrime. In practice, efforts to combat cybercrime frequently encounter socio-technical obstacles, particularly regarding the identification of perpetrators and the seizure of evidence. The lack of oversight and the absence of mandatory registration regulations for users of public facilities—such as internet cafes—often cause the tracing

E-ISSN: 3032-0135
Vol. 4, No.1, July - December (2026), pp. 371 - 377

of digital footprints to hit a dead end at an anonymous IP address, without any eyewitnesses with direct knowledge. The phenomenon of personal data hacking is becoming increasingly diverse; the Cyber Crime Investigation Directorate of the Bali Regional Police has noted that the most prevalent forms of such crimes currently include unauthorized access, malware distribution, credential theft, phishing, and the exploitation of One-Time Password (OTP) codes.

The complexity of investigations is mounting due to the cross-regional and transnational nature of cybercrimes. Perpetrators typically operate outside the local jurisdiction of the Bali Regional Police, employing identity-masking technologies—such as Virtual Private Networks (VPNs) and proxy servers—and using false identities to complicate digital tracking. Law enforcement challenges become significantly more complex when the digital platforms or server infrastructure utilized by perpetrators are located abroad. This situation compels investigators to rely on bureaucratic international cooperation mechanisms, such as Mutual Legal Assistance (MLA), while simultaneously requiring advanced digital forensic capabilities to analyze electronic evidence in compliance with criminal procedural law.

When analyzed through the lens of Lawrence M. Friedman's legal system theory, this dilemma reveals simultaneous obstacles across the three primary legal subsystems. Regarding legal structure, although the Cyber Crime Investigation Directorate of the Bali Regional Police has assembled a team of competent forensic personnel, the transnational nature of cybercrime prevents law enforcement from operating in isolation; instead, it relies heavily on cross-sectoral and international coordination. From the perspective of legal substance, despite Indonesia's efforts to safeguard cyberspace through Law No. 1 of 2024 (the Second ITE Law) and Law No. 27 of 2022 (the Personal Data Protection Law), conflicts arising from differing international legal systems and the rapid pace of technological evolution remain significant normative challenges. These difficulties are compounded by a legal culture characterized by low public awareness regarding digital threats—such as phishing schemes and OTP security—thereby underscoring that successful cyber law enforcement hinges on the integration of regulations, the strengthening of law enforcement agencies, and the enhancement of public legal awareness.

2.3 Efforts by the Cyber Crime Investigation Directorate of the Bali Regional Police in Enforcing the Law Against the Crime of Personal Data Hacking

The emergence of social media as a space for global public interaction has not only bridged geographical distances but also given rise to new vulnerabilities in the form of deviant behavior in cyberspace. The open nature of internet-based information networks has fueled a massive escalation in cybercrime, paralleling the growing number of technology users. In response to these dynamics, the

E-ISSN: 3032-0135
Vol. 4, No.1, July - December (2026), pp. 371 - 377

Cyber Crime Investigation Directorate of the Bali Regional Police is consolidating its law enforcement strategy by strengthening its *pro-justitia* investigative capabilities. At the tactical level, the police are optimizing the use of specialized equipment and materials to facilitate digital analysis, profiling, Open-Source Intelligence (OSINT), and digital forensics, thereby securing digital traces and obtaining admissible electronic evidence in accordance with criminal procedural law.

Given the borderless nature of cybercrime—which frequently involves infrastructure located outside national jurisdictions—the Cyber Crime Investigation Directorate of the Bali Regional Police employs a case-handling approach rooted in institutional interconnection. This strategy is implemented through intensive collaboration with various stakeholders, including telecommunications operators, the Ministry of Communication and Digital (Komdigi), the National Cyber and Crypto Agency (BSSN), the banking sector, and digital platform providers. Such synergy aims to accelerate the tracing of digital identities and the securing of electronic evidence—efforts that are further bolstered on a transnational scale through international cooperation mechanisms. Furthermore, internal capabilities are continuously enhanced through certification, improved cyber literacy, strengthened early detection, and the refinement of preventive measures—such as regular cyber patrols—designed to minimize the convergence of intent and opportunity for hackers.

When analyzed through the lens of Lawrence M. Friedman's legal system theory, the commitment of the Bali Regional Police's Cyber Crime Directorate (Ditressiber Polda Bali) to combating personal data hacking reflects a robust integration of the three legal subsystems. Regarding the legal structure component, institutional capacity building is evidenced by enhanced investigator competence, the utilization of specialized forensic equipment, and the establishment of cross-sectoral and transnational collaborative coordination networks. In terms of legal substance, the legality of evidence gathering and investigative operations rests upon a clear normative framework—including Law No. 1 of 2024 (the Second ITE Law), Law No. 27 of 2022 (the Personal Data Protection Law), the Criminal Procedure Code (KUHAP), and internal National Police regulations—thereby ensuring adherence to the principle of due process of law. Finally, regarding legal culture, the law enforcement orientation has shifted toward prevention through cyber patrols and digital literacy initiatives aimed at fostering public legal awareness regarding personal data protection. The synergy among these three elements serves as a primary determinant in ensuring legal certainty, protecting privacy rights, and building public trust in the performance of the Bali Regional Police's Cyber Crime Directorate.

Conclusion

Law enforcement regarding the crime of personal data hacking by the Bali Regional Police's Cyber Investigation Directorate has operated effectively and in accordance with regulations through

E-ISSN: 3032-0135
Vol. 4, No.1, July - December (2026), pp. 371 - 377

an integrated approach combining repressive measures—such as investigations and digital forensics—with preventive efforts like cyber patrols and public education; this strategy has successfully reduced the trend of such cases between 2024 and May 2026. Drawing on the theories of Philipus M. Hadjon and Lawrence M. Friedman, the success of this legal protection is heavily influenced by the alignment of legal structure, substance, and culture. Despite facing complex challenges—such as the transnational nature of the crimes, perpetrator anonymity, and the need to trace overseas servers—the Bali Regional Police have addressed these issues by enhancing investigator competence, utilizing specialized equipment, and strengthening national and international synergy. Through the continuous reinforcement of these legal system components, it is expected that law enforcement and the protection of public personal data will continue to be optimized in an integrated manner.

REFERENCES

BOOKS AND JOURNALS

Arisandy, Yogi Oktafian. 2019. Criminal Law Enforcement Against Cybercrime. Jakarta: Media Ilmu.

Hartono, Bambang. 2013. "Imposition of Criminal Sanctions for the Crime of Carding". Pranata Hukum, Faculty of Law, Universitas Bandar Lampung, Vol. 8, No. 2.

Prasetiyo and Mukhtar Zuhdy. 2020. "Law Enforcement by Cybercrime Investigators Regarding Cybercrime within the Jurisdiction of the DIY Regional Police". Indonesian Journal of Criminal Law and Criminology (IJCLC), Faculty of Law, Universitas Muhammadiyah Yogyakarta, Vol. 1, No. 2.

LEGISLATION

The 1945 Constitution of the Republic of Indonesia.

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.

Regulation of the Indonesian National Police Number 8 of 2021 concerning the Handling of Criminal Acts Based on Restorative Justice.

INTERVIEW (PRIMARY DATA)

Interview with Police Brigadier Ni Made Septiwidiantari, S.H., M.H., Administrative Officer, Sub-directorate 1, Cyber Investigation Directorate, Bali Regional Police, on Tuesday, June 30, 2026.

Interview with Police Commissioner Adjutant I Made Martadi Putra, S.Kom., M.T., M.Sc., Head of Unit 1, Sub-directorate III, Cyber Investigation Directorate, Bali Regional Police, on Tuesday, June 30, 2026.