FAKULTAS HUKUM
UNIVERSITAS MUSLIM INDONESIA

Al-Ishlah: Jurnal Ilmiah Hukum
P-ISSN: 1410-9328 || E-ISSN: 2614-0071
https://jurnal.fh.umi.ac.id/index.php/ishlah/article/view/v28n1-1
Vol. 28 Issue 2 : June 2025 – November 2025. Published Online: Juni - November, 2025

Article Title

Criminal Law Enforcement on Illegal Access to Bank Customer Data: A Study at the South Sulawesi Regional Police

Author (s)

Dodik Susianto
Magister of Law, Universitas Muslim Indonesia, Indonesia
Emal: dodik.susianto@umi.ac.id

La Ode Husen
Faculty of Law, Universitas Muslim Indonesia, Indonesia
Emal: laode.husen@umi.ac.id

Zainuddin
Faculty of Law, Universitas Muslim Indonesia, Indonesia
Emal: zainuddin.zainuddin@umi.ac.id

Muh. Zulkifli Muhdar
Faculty of Law, Universitas Muslim Indonesia, Indonesia
Emal: muhzulkifli.muhdar@umi.ac.id

How to cite:

Susianto, D., Husen, L. O., Zainuddin, Z. & Muhdar, M. Z. (2026). Criminal Law Enforcement on Illegal Access to Bank Customer Data: A Study at the South Sulawesi Regional Police. 29(1), Al-Ishlah: Jurnal Ilmiah Hukum, 29(1), 198-212.

ABSTRACT

This study aims to analyze criminal law enforcement against perpetrators of illegal access to bank customer data at the South Sulawesi Regional Police and to identify the factors influencing its effectiveness. The research employs an empirical legal method with a normative-empirical approach, examining the relationship between legal norms and their implementation in practice. Data were collected through library research, interviews, and document studies, using both primary and secondary legal materials. The findings reveal that criminal law enforcement has been implemented through investigation and inquiry processes based on the Law on Information and Electronic Transactions, the Banking Law, and the Personal Data Protection Law. However, its effectiveness has not yet been fully optimal due to several obstacles, including limited human resource capacity, inadequate digital forensic facilities, the complexity of electronic evidence, weak inter-agency coordination, rapid technological developments, and low public awareness of digital security. The study concludes that strengthening adaptive regulations, improving investigator competence, enhancing digital forensic infrastructure, and intensifying coordination among law enforcement agencies, banking institutions, and regulatory bodies are essential to achieving more effective and professional law enforcement. Public education on personal data protection is also necessary to support preventive efforts against cybercrime in the banking sector.

Keywords: Criminal Law Enforcement; Illegal Access; Bank Customer Data; Cybercrime

INTRODUCTION

The development of information and communication technology has brought about major transformations in various aspects of modern life. These transformations have not only influenced patterns of social interaction but have also fundamentally changed economic and financial systems (Amory & Mudo, 2025). The banking sector has become one of the fields experiencing massive digitalization through the use of internet-based technology. Services such as mobile banking, internet banking, and digital payment systems provide easier access for the public in conducting financial transactions (Dz, 2018), This convenience has encouraged increased financial inclusion across various levels of society. This development has simultaneously increased dependence on electronic systems in managing financial data. Such dependence ultimately gives rise to new challenges related to the security and protection of customer data (Mukhra, *et al,* 2024).

Banking digitalization creates an efficient ecosystem but is vulnerable to cybersecurity threats. Globally connected electronic systems open opportunities for irresponsible parties to carry out illegal access (Fonda & Hoesein, 2025). Customer data becomes a primary target because it holds high economic value in cybercrime practices. Information such as account numbers, personal identities, and transaction histories can be misused for various criminal activities (Antoine, *et al,* 2025). These risks continue to increase along with the complexity of technological systems used by financial institutions. Security system weaknesses can be exploited through increasingly sophisticated hacking techniques. This condition shows that data security has become a crucial issue in the modern banking industry (Sari, Istan & Hendrianto, 2025).

The principle of bank secrecy is a fundamental foundation in maintaining public trust in banking institutions. Public trust heavily depends on the ability of banks to protect customer data and information (Zahro Zahra & Faidhah, 2024). Indonesian positive law has regulated the obligation of banks to maintain the confidentiality of customer data. These provisions are reflected in regulations that prohibit disclosure of data without a lawful basis (Aziz, 2025). Violations of this principle can seriously impact the reputation of banking institutions. Public trust may decline in the event of massive data breaches. The stability of the financial system may also be disrupted due to the loss of public confidence (Rinaldi & Wijaya, 2025).

The phenomenon of illegal access to bank customer data has shown a significant increase in recent years. The modus operandi used by perpetrators has become increasingly diverse and complex (Rahman, 2025). Techniques such as phishing, malware, social engineering, and insider threats are commonly used to gain access to banking systems. Perpetrators are not only external actors but may also involve internal parties (Hassandi & Pangestu, 2025). Insider involvement poses a serious threat because of direct access to data systems. This situation indicates that security depends not only on technology but also on the integrity of human resources. This complexity requires a multidimensional approach in handling such crimes (Hoshmand & Ratnawati, 2023).

Illegal access to customer data falls under the category of cybercrime, which has unique characteristics. This type of crime is transnational and difficult to trace due to its reliance on global networks (Firdaus, 2024). Perpetrators may operate from locations different from the victims, even across jurisdictions. This condition creates difficulties in law enforcement processes (Kuba, 2022). Law enforcement officers must possess technical capabilities and cross-border coordination. Evidence in cybercrime cases requires complex digital forensic approaches. These characteristics distinguish cybercrime from conventional crimes (Handayani, Hidayat & Saputra, 2025).

Losses resulting from illegal access to customer data are not only material. Non-material impacts such as loss of trust and sense of security are also significant consequences. Customers may suffer financial losses due to account breaches (Nashrullah & Mustofa, 2025). Stolen personal identities may be used for fraud or other crimes. The domino effect of such crimes can damage the reputation of financial institutions. Broader impacts may disrupt the stability of the national financial system (Rusyiana, Ardiyanto & Anam, 2025). Therefore, the protection of customer data becomes a top priority in legal policy.

The legal framework in Indonesia has provided a normative basis for addressing illegal access to electronic data. Laws governing information and electronic transactions serve as the main instruments in law enforcement. These provisions prohibit any person from accessing electronic systems without authorization. Criminal sanctions are imposed on perpetrators as a form of legal protection. These regulations demonstrate the state's commitment to addressing technology-based crimes. However, implementation in practice still faces various challenges. The effectiveness of law enforcement remains an issue that needs in-depth study (Aprilianti, 2024).

Regulations concerning personal data protection have also been strengthened through recent legislation. Personal data protection is an important aspect of safeguarding individual privacy rights. Bank customer data falls into the category of data that must be strictly protected. These regulations cover the processes of data collection, processing, and storage. Violations of these provisions may result in administrative and criminal sanctions. Implementation of these regulations still faces practical challenges. The gap between normative provisions and reality remains a problem that needs analysis.

The rapid development of technology is often not matched by the readiness of legal regulations. Law tends to be reactive to technological advancements. This condition creates legal loopholes that can be exploited by criminals. Law enforcement officers face difficulties in adapting to technological developments. Limited technical understanding is one of the main obstacles. Regulatory reform becomes an urgent necessity in addressing cybercrime dynamics. An adaptive legal approach is required to meet these challenges.

Criminal law enforcement plays a strategic role in combating illegal access to customer data. The law enforcement process includes investigation, inquiry, and prosecution stages. The police hold primary authority in handling cybercrime cases. The capability of officers in uncovering cases greatly determines the success of law enforcement. Support in terms of technology and human resources is essential. Coordination among institutions is also necessary in handling cross-sector crimes. The effectiveness of law enforcement becomes an indicator of the success of the criminal justice system.

The South Sulawesi Regional Police have an important role in handling cybercrime in their jurisdiction. This region has experienced an increase in the use of digital banking services. This increase is aligned with the potential for illegal access crimes. Case handling requires a professional and technology-based approach. Specialized cyber units are responsible for managing such cases. The performance of law enforcement officers determines the realization of justice. Research on law enforcement practices is therefore important.

The complexity of evidence in cybercrime cases becomes a major challenge for law enforcement officers. Digital evidence has different characteristics compared to conventional evidence. Its validity and authenticity must be legally accountable. Digital forensic processes require special expertise and advanced equipment. Limited facilities may hinder investigation processes. Officers must keep up with technological developments used by perpetrators. This challenge highlights the importance of strengthening institutional capacity.

Limitations in human resources pose obstacles in handling cybercrime. Not all officers have competencies in information technology. Specialized training and education become urgent needs. Capacity building must be carried out continuously. The quality of law enforcement depends heavily on the competence of officers. Budget support is also an important factor in capacity development. Without such support, effective law enforcement will be difficult to achieve.

Cases of customer data breaches in Indonesia indicate weaknesses in security systems. Several major incidents have attracted public and governmental attention. Large-scale data

breaches show vulnerabilities in protection systems. Perpetrators can exploit these weaknesses for personal gain. The impact of such cases creates public anxiety. Trust in the banking system declines. This condition demands comprehensive improvements in security systems.

Cyberattacks on financial institutions also demonstrate serious threats to digital systems. Banking services may be disrupted due to such attacks. Economic activities of society may be affected by system failures. These incidents highlight the importance of strong security systems. Investment in cybersecurity technology becomes unavoidable. Financial institutions must anticipate evolving threats. System protection becomes part of institutional responsibility.

Effective law enforcement requires synergy among various stakeholders. Government, law enforcement agencies, and the private sector must collaborate. This collaboration is crucial in addressing complex crimes. Information sharing becomes key in solving cases. International cooperation is also needed in cross-border cases. A collaborative approach can enhance effectiveness in handling crimes. Such synergy is part of the national cybersecurity strategy.

Legal protection of customer data does not rely solely on regulations. Public awareness also plays an important role in preventing crime. Education on digital security needs to be improved. Customers must understand risks in using digital services. Safe behavior can reduce the potential for crime. Public participation becomes part of the protection system. Preventive approaches must go hand in hand with law enforcement.

Research on law enforcement against illegal access to customer data has high relevance. This study can provide an overview of legal effectiveness in practice. Analysis of obstacles can serve as a basis for policy improvement. Research also contributes academically to the development of legal science. The results are expected to provide constructive recommendations. An empirical approach is necessary to understand field realities. This study becomes important in the context of technological development.

Focusing research on the South Sulawesi Regional Police provides specific value in analysis. This region has unique social and technological dynamics. Case handling at the regional level may reflect national conditions. Empirical data from the field becomes an important source of information. Analysis of law enforcement practices provides concrete insights. Research findings can be used for evaluation purposes. This approach contributes practically to policy development.

The issue of illegal access to bank customer data is complex and multidimensional. Legal, technological, and social aspects are interconnected in this problem. A comprehensive approach is required in addressing it. Law enforcement must be able to respond to technological challenges. Protection of society remains the primary objective. The legal system must be adaptive to changing times. This research is expected to contribute meaningfully to these efforts.

METHOD

This study employs an empirical legal research method with a normative-empirical approach that examines the relationship between legal norms (das sollen)

and their implementation in practice (das sein). The focus of the study is directed toward analyzing criminal law enforcement against perpetrators of illegal access to bank customer data, particularly cases handled by the South Sulawesi Regional Police as the primary institution in the investigation process. The research location is selected purposively based on the consideration of the police's authority as law enforcement officers directly involved in handling criminal cases based on information technology. The data sources used consist of primary and secondary data that complement each other in the analysis process. Primary data are obtained through interviews with police investigators and law enforcement officers who have experience in handling relevant cases. Secondary data are collected through library research, including statutory regulations, academic literature, journals, and relevant legal documents. The combination of these two types of data aims to provide a comprehensive overview of the effectiveness of law enforcement in practice.

Data collection techniques are carried out through library research, interviews, and document studies to obtain valid and in-depth information related to the practice of criminal law enforcement against illegal access to bank customer data. Interviews are conducted in both structured and semi-structured forms to explore information regarding investigative procedures, legal considerations, and the obstacles faced by law enforcement officers. The sampling method uses purposive sampling by selecting informants who possess relevant competence and experience in the field under study. The collected data are analyzed using qualitative methods through stages of legal material inventory, classification and substantive analysis, and processing of empirical data. The analysis is conducted by integrating normative and empirical findings to obtain a comprehensive understanding of the research problem. The conclusion is drawn deductively by linking legal theory with field facts. This approach is expected to produce findings that are not only descriptive but also provide prescriptive recommendations for strengthening law enforcement in the field of cybercrime.

RESULT AND DISCUSSION

A. Criminal Law Enforcement Against Perpetrators of Illegal Access to Bank Customer Data by the South Sulawesi Regional Police

Criminal law enforcement against perpetrators of illegal access to bank customer data by the South Sulawesi Regional Police demonstrates complex dynamics in practice. Investigators from the Directorate of Special Criminal Investigation hold primary authority in handling cybercrime cases. The case-handling process begins from the investigation stage to the inquiry stage, requiring in-depth analysis of digital evidence. Such evidence includes server logs, IP addresses, and electronic transaction records. Technical expertise becomes a crucial factor in uncovering these crimes. Investigators must be able to interpret complex digital data. This condition indicates that law enforcement is not only based on legal norms but also on technical capability.

The investigation process for illegal access to bank customer data generally begins with reports from victims or banking institutions. These reports serve as the

basis for investigators to collect initial evidence. This stage includes identifying crime patterns and tracking the digital activities of perpetrators. Investigators coordinate with banks to obtain relevant data. This process requires a high level of accuracy to avoid misinterpretation of data. The evidence obtained must meet legal standards to be admissible in court. This initial stage determines the success of subsequent legal proceedings.

The phenomenon of illegal access to bank customer data has shown a significant increase in recent years. Perpetrators exploit weaknesses in system security to gain unauthorized access. Techniques used include phishing, malware, and credential theft. The complexity of these methods creates difficulties in identifying perpetrators. Digital traces are often concealed using certain technologies. This condition illustrates that cybercrime continues to evolve dynamically. Law enforcement must be able to keep up with these developments.

The use of malware and social engineering techniques poses serious challenges in investigating cybercrime cases. Perpetrators can deceive victims into voluntarily providing sensitive information. This information is then used to access banking systems. Investigators must be able to identify the attack patterns used by perpetrators. The analysis of digital evidence requires accurate forensic approaches. Errors in analysis can affect investigation outcomes. Precision becomes key in this process.

The legal basis for enforcing cases of illegal access to bank customer data refers to the Law on Information and Electronic Transactions and the Criminal Code. These legal provisions provide a foundation for investigators to prosecute perpetrators. Articles regulating illegal access serve as primary instruments in law enforcement. Legal application must be carried out accurately to avoid misinterpretation. Investigators must understand the substance of the law comprehensively. The integration of law and technology becomes essential in such cases. Legal certainty remains the main objective of enforcement.

The evidentiary process in illegal access cases has a high level of complexity. Electronic evidence has different characteristics compared to conventional evidence. The validity of evidence must be legally accountable. Investigators must ensure that evidence has not been manipulated. Digital forensic processes become an essential part of proof. Limited facilities may hinder this process. This indicates the need for improved technological infrastructure.

Limitations in human resources become one of the main obstacles in enforcing cybercrime laws. Not all investigators possess competence in information technology. Specialized training becomes an urgent necessity for law enforcement officers. Capacity building must be carried out continuously. The quality of investigation depends heavily on the competence of individual investigators. Institutional support

plays an important role in developing competence. Without such improvement, effective law enforcement is difficult to achieve.

The cybercrime unit established by the South Sulawesi Regional Police has contributed to handling such cases. This unit has a specific function in dealing with technology-based crimes. Its existence improves responsiveness to public reports. However, limited capacity becomes an obstacle in case handling. The number of cases continues to increase while the number of investigators remains limited. This condition results in longer investigation processes. The effectiveness of case handling needs to be improved.

Coordination between the police and banking institutions is a key factor in law enforcement. Data held by banks serves as the main source in investigations. Good cooperation can accelerate case resolution. Lack of coordination can hinder evidence collection. Integration of information systems becomes necessary to support investigations. Cross-sector collaboration must be strengthened. This synergy is key to successful law enforcement.

Illegal access cases often involve perpetrators operating across regions and even across countries. This condition creates challenges in law enforcement processes. Investigators must coordinate with authorities in other regions. Cross-jurisdictional legal procedures become a separate challenge. International cooperation becomes necessary in certain cases. Without proper coordination, legal processes may be obstructed. Case handling requires a global approach.

Court decisions in cybercrime cases show variations in the application of law. Some cases result in minimal sentences due to difficulties in proof. Digital evidence is often difficult to verify with absolute certainty. Judges require conviction supported by valid legal evidence. This uncertainty affects the effectiveness of law enforcement. Standards of proof need to be clarified in regulations. Legal certainty must become a priority in the judicial system.

Comparisons with other regions show differences in the effectiveness of law enforcement. Police units in major cities have more complete facilities. Digital forensic laboratories serve as key supporting factors. Investigations can be conducted more quickly and accurately. South Sulawesi still faces limitations in facilities. Improvement of infrastructure becomes an urgent need. Equal capacity is important in the national system.

The impact of illegal access to customer data is not only financial. Customers suffer material losses due to loss of funds. Psychological impacts are also experienced by victims. Trust in the banking system declines. This may affect the stability of the financial sector. Legal protection becomes a necessity for the public. Law enforcement must provide a sense of justice.

Banks bear responsibility for maintaining the security of data systems. Implementation of security technology becomes a preventive measure. Systems such as multi-factor authentication can reduce the risk of crime. Security audits must be conducted periodically. System weaknesses must be promptly addressed. Investment in technology becomes a primary necessity. Data security becomes a priority for banking institutions.

Public awareness of digital security becomes an important factor in crime prevention. Education on cybercrime risks needs to be enhanced. Customers must understand how to protect their personal data. Safe behavior can reduce potential crime. Public participation becomes part of the protection system. Prevention becomes an effective strategy. Law enforcement must be supported by public awareness.

The use of advanced technology can assist investigators in solving cases. Artificial intelligence can be used to analyze crime patterns. Machine learning helps detect suspicious activities. Blockchain tracing can track digital transactions. These technologies improve investigation efficiency. Integration of technology becomes essential in law enforcement. System modernization becomes a strategic step.

Preventive and repressive approaches must be balanced in law enforcement. Punishment of perpetrators provides a deterrent effect. Prevention through education can reduce the number of cases. A combined strategy becomes an effective approach. Legal policies must accommodate both aspects. Protection of society remains the primary objective. The legal system must be adaptive to change.

Legal regulations must be updated to keep pace with technological developments. Provisions regarding digital evidence must be clarified. Standards of proof must be aligned with technological advancements. Legal certainty becomes an important factor in law enforcement. Regulatory updates must be carried out periodically. Involvement of various stakeholders is necessary in this process. Legal reform becomes an urgent necessity.

Improving investigator capacity becomes a strategic step in addressing cybercrime. Training and certification must be provided continuously. Technical competence becomes a key factor in investigation. Institutional support must be maximized. Investment in human resources becomes a priority. The quality of law enforcement depends on the capability of officers. Professionalism becomes the key to success.

Law enforcement against illegal access to bank customer data in South Sulawesi shows progress. Technical and regulatory obstacles remain major challenges. Improvement efforts must be carried out comprehensively. Synergy between technology, law, and human resources becomes essential. A multidimensional approach is required in case handling. The effectiveness of law enforcement must

continue to be improved. The legal system must be able to provide optimal protection for society.

B. Factors Influencing Criminal Law Enforcement Against Perpetrators of Illegal Access to Bank Customer Data by the South Sulawesi Regional Police

Criminal law enforcement against perpetrators of illegal access to bank customer data by the South Sulawesi Regional Police is influenced by various interrelated factors. These factors include legal aspects, institutional capacity, technology, and community behavior. The complex characteristics of cybercrime require an adaptive and multidimensional law enforcement approach. Illegal access to bank customer data involves sophisticated electronic systems and extensive digital networks. This crime not only causes financial losses but also undermines public trust. These conditions require law enforcement officers to work professionally and be technology-oriented. The effectiveness of law enforcement is largely determined by the ability to manage these factors.

The substance of the law becomes the primary factor in determining the direction of criminal law enforcement. Regulations governing illegal access to bank customer data provide a normative basis for law enforcement officers. The Law on Information and Electronic Transactions, the Banking Law, and the Personal Data Protection Law serve as the main legal foundations. The existence of these regulations reflects the state's commitment to protecting customer data. Implementation of regulations often faces challenges due to differing interpretations. Harmonization among regulations has not been fully optimal in practice. Legal certainty remains a challenge in the application of these norms.

The quality of law enforcement officers has a significant influence on the effectiveness of law enforcement. Investigators must possess technical competence in information technology and digital forensics. The ability to analyze electronic evidence is a fundamental requirement in solving cases. Without such competence, the evidentiary process will encounter obstacles. Specialized training and education become unavoidable necessities. Professionalism of officers serves as an indicator of successful law enforcement. Strengthening human resource capacity must be carried out continuously.

The availability of facilities and infrastructure is an important factor in supporting law enforcement. Digital forensic tools are required to analyze electronic evidence accurately. Digital forensic laboratories serve as primary facilities in uncovering cybercrime cases. Limitations in technology can slow down the investigation process. Procurement of data analysis software becomes a strategic necessity. Facility support must align with technological developments. Without adequate infrastructure, law enforcement cannot function optimally.

Inter-agency coordination is a determining factor in the effectiveness of law enforcement. The police must collaborate with banking institutions and regulatory agencies. Transaction data and banking security systems serve as primary sources in investigations. Lack of coordination can hinder evidence collection. Integration of information across institutions becomes an urgent necessity. Cross-sector collaboration must be strengthened. Such synergy will accelerate case handling.

The development of information technology influences the complexity of crimes. Perpetrators' modus operandi becomes increasingly sophisticated alongside technological advancement. Techniques such as phishing and malware continue to evolve. Perpetrators exploit system vulnerabilities to gain illegal access. Law enforcement officers must keep pace with these developments. Technological lag will become an obstacle in law enforcement. Adaptation to technology becomes essential.

Public awareness of digital security plays a significant role in crime prevention. Many cases occur due to users' negligence in protecting personal data. Sensitive information is often shared without adequate security considerations. This condition is exploited by perpetrators. Public education becomes a strategic measure. Safe behavior can reduce crime risks. Community participation supports the effectiveness of law enforcement.

Internal banking security systems also influence the level of illegal access crimes. Banks are responsible for safeguarding customer data. System weaknesses can be exploited by criminals. Security audits must be conducted periodically. Implementation of security technology becomes a priority. Internal supervision must be strengthened. A robust system will minimize crime potential.

Evidentiary processes in criminal law pose major challenges in cybercrime cases. Electronic evidence has complex and technical characteristics. The validity of evidence must be ensured through digital forensic processes. Investigators must understand evidence collection procedures. Errors in evidence handling can have serious consequences. Standards of proof must be clarified in regulations. Legal certainty becomes the main objective in evidence assessment.

Government policy support greatly determines the success of law enforcement. The government plays a role in providing regulations and funding. Strengthening law enforcement capacity becomes part of national policy. Coordination among institutions must be facilitated by the government. Without policy support, law enforcement efforts will be constrained. Government commitment becomes a key factor. Appropriate policies will enhance the effectiveness of law enforcement.

The structure of the legal system also affects law enforcement processes. Police, prosecutors, and courts must operate in an integrated manner. Case transfer processes require proper coordination. Administrative constraints often become obstacles. Legal processes may take longer due to suboptimal coordination. System integration

becomes necessary in criminal justice. Effectiveness depends on inter-agency coordination.

Law enforcement theory indicates that effectiveness is influenced by multiple factors. Legal factors, law enforcement officers, facilities, society, and legal culture are interconnected. These five factors must operate in balance. Imbalance in one factor will affect law enforcement outcomes. Theoretical approaches provide comprehensive analytical foundations. Law enforcement must be viewed systemically. Integration of factors becomes the key to success.

Legal culture within society is a significant factor. Public attitudes toward the law influence compliance levels. Low legal awareness can hinder law enforcement. Many cases remain unreported for various reasons. Reluctance to report becomes a barrier to case disclosure. Improving legal culture becomes necessary. Legal awareness must be built through education.

The complexity of cybercrime continues to increase alongside technological development. Perpetrators may be individuals or organized groups. International networks are often used to conceal identities. Investigators must have the capability to handle transnational crimes. International cooperation becomes necessary. A global approach is required in case handling. This complexity demands adaptive law enforcement strategies.

Limitations in authority to access banking data become obstacles in investigations. The principle of bank secrecy restricts access to customer data. Investigators must follow legal procedures. Authorization processes often take considerable time. This condition can slow down investigations. Balance between confidentiality and law enforcement must be maintained. Regulations must provide clarity in this regard.

The role of cybercrime units is crucial in handling cases. These units have specific duties in addressing technology-based crimes. Limited personnel poses a challenge. High workloads affect handling effectiveness. Strengthening organizational structures becomes necessary. Increasing personnel is required. Strong units will improve law enforcement quality.

Support from digital forensic technology is essential in the evidentiary process. Analysis of electronic evidence requires scientific approaches. Digital data must be verified accurately. Without adequate technology, proof becomes difficult. Investment in technology becomes a necessity. System modernization must be implemented. Technology serves as the primary tool in cybercrime law enforcement.

Funding is an important factor in supporting law enforcement. Handling cybercrime cases requires substantial costs. Procurement of technology and training requires budget allocation. Limited funding can hinder law enforcement processes.

Government must provide financial support. Budget management must be conducted effectively. Adequate funding will improve institutional performance.

Criminal policy approaches become strategic in crime prevention. Law enforcement is not solely repressive. Preventive measures are equally important. Digital security awareness campaigns must be intensified. Cooperation with banking institutions becomes strategic. A comprehensive approach enhances effectiveness. Policies must include preventive and repressive aspects.

A victim-oriented approach is important in law enforcement. Protection of customers must be prioritized. Victims must receive adequate recovery. The legal system must ensure protection guarantees. This approach increases public trust. Law enforcement must be justice-oriented. Victim protection becomes part of the legal system.

Criminal liability in cybercrime cases often becomes a subject of debate. Determining the main perpetrator is not always straightforward. Internal and external actors may be involved. Legal analysis must be conducted thoroughly. Elements of fault must be clearly proven. This complexity requires a multidisciplinary approach. Law enforcement must address these challenges effectively.

Technical regulations regarding electronic evidence still need strengthening. Standards for evidence collection and storage must be clear. Without such standards, evidence may be disputed in court. Legal certainty becomes essential. Investigators must follow proper procedures. Regulatory reform becomes urgent. This will enhance law enforcement quality.

Internal banking supervision plays a role in supporting law enforcement. Effective supervision facilitates identification of perpetrators. Banks must report any indications of violations. Institutional responsibility must be carried out optimally. Cooperation with law enforcement is essential. Effective supervision accelerates legal processes. Strong systems enhance data security.

The security of banking digital systems becomes a primary preventive factor. Strong systems reduce opportunities for crime. Police must understand the technologies used by banks. System analysis becomes part of investigation. Collaboration with technology experts is necessary. Technical approaches are essential. Law enforcement cannot be separated from technology.

International cooperation becomes an important factor in addressing cybercrime. Crimes often involve global networks. Investigators must collaborate with international agencies. Cross-border legal procedures must be understood. Without cooperation, perpetrators are difficult to apprehend. A global approach becomes necessary. International collaboration enhances law enforcement effectiveness.

Public trust in the police and banking institutions becomes a critical factor. Transparent law enforcement increases public confidence. Professionalism of officers becomes the main key. Public trust influences community participation. The legal system must ensure certainty and justice. Without trust, law enforcement is ineffective. Transparency and accountability become fundamental principles.

CONCLUTION AND SUGGESTIONS

Criminal law enforcement against perpetrators of illegal access to bank customer data by the South Sulawesi Regional Police has been implemented but has not yet reached optimal effectiveness due to various influencing factors, including limitations in human resource capacity, digital forensic technological facilities, the complexity of electronic evidence, and suboptimal inter-agency coordination, in addition to external factors such as low public awareness and the rapid development of cybercrime technologies; therefore, it is recommended to strengthen regulations that are more adaptive to technological developments, enhance investigators' competencies through training and cybercrime certification, provide adequate digital forensic infrastructure, improve coordination among the police, banking institutions, and related agencies, and strengthen public education on personal data security in order to establish a more effective, professional law enforcement system capable of providing optimal legal protection for banking customers.

REFERENCES

Antoine, R. A., Farizqa, N. S., Hasna, A. H., & Pasaribu, M. (2025). Penyalahgunaan Data Pribadi dalam Teknologi Transaksi Digital di Industri Perbankan Digital (Studi Kasus PT. Bank Syariah Indonesia). *Jurnal Multidisiplin Ilmu Akademik*, *2*(1), 316-327.

Amory, J. D. S., & Mudo, M. (2025). Transformasi ekonomi digital dan evolusi pola konsumsi: Tinjauan literatur tentang perubahan perilaku belanja di era internet. *Jurnal Minfo Polgan*, *14*(1), 28-37.

Aprilianti, A. (2024). Efektivitas dan implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai hukum siber di Indonesia: Tantangan dan solusi. *Begawan Abioso*, *15*(1), 41-50.

Aziz, M. F. (2025). Perlindungan Hukum terhadap Nasabah atas Penyalahgunaan Data Pribadi oleh Pihak Bank di Era Digitalisasi Perbankan. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *3*(6), 8840-8852.

Dz, A. S. (2018). Inklusi keuangan perbankan syariah berbasis digital-banking: Optimalisasi dan tantangan. *Al-Amwal: Jurnal Ekonomi dan Perbankan Syari'ah*, *10*(1), 63-80.

Firdaus, R. A. (2024). Perlindungan hukum dan pencegahan kejahatan siber di era digital dalam sistem hukum di Indonesia. *STAATSRECHT: Jurnal Hukum Kenegaraan dan Politik Islam*, *4*(1), 79-104.

Fonda, H., & Hoesein, Z. A. (2025). Pertanggungjawaban Bank dalam Menjamin Keamanan Data Nasabah di Era Digitalisasi Perbankan. *Jurnal Retentum*, *4*(1), 34-47.

Handayani, A., Hidayat, S., & Saputra, D. N. (2025). Penegakan hukum terhadap praktik judi online di era digital: Studi kasus cyber crime di Indonesia. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *3*(2), 207-215.

Hassandi, I., & Pangestu, M. G. (2025). Identifikasi Resiko Dalam Era Digital: Studi Kasus Resiko Teknologi Pada PT Bank Syariah Indonesia. *Jurnal Manajemen Teknologi Dan Sistem Informasi (JMS)*, *5*(1), 996-1004.

Hoshmand, M. O., & Ratnawati, S. (2023). Analisis keamanan infrastruktur teknologi informasi dalam menghadapi ancaman cybersecurity. *Jurnal Sains Dan Teknologi*, *5*(2), 679-686.

Kuba, S. (2022). Optimalisasi Perlindungan Saksi dan Korban Dalam Rangka Memantapkan Penegakan Hukum Di Indonesia. *Jurnal Kajian Ilmiah*, *22*(1), 89-100.

Mukhra, U. H., Makruf, J. J., Kesuma, T. M., Nizam, A., & Siregar, M. R. (2024). *Mobile Banking Dalam Persepsi Privasi Nasabah*. Syiah Kuala University Press.

Nashrullah, M. N., & Mustofa, I. (2025). Implementasi Konsep Keadilan Terhadap Perlindungan Konsumen (Studi Kasus: Serangan Cyber kepada Data Nasabah Bank Syariah Indonesia). *Jurnal Hukum Ekonomi Syariah*, *8*(1), 15-30.

Rahman, M. S. F. (2025). Kajian Kriminologis Terhadap Motif dan Modus Operandi Tindak Pidana Perubahan Data di Indonesia. *HARISA: Jurnal Hukum, Syariah, dan Sosial*, *2*(1)), 81-95.

Rinaldi, F. A., & Wijaya, B. K. (2025). Efektivitas Penegakan Hukum terhadap Tindak Pidana Perbankan: Studi Kasus Pembobolan Dana Nasabah. *PENG: Jurnal Ekonomi Dan Manajemen*, *2*(3), 3437-3447.

Rusyiana, R., Ardiyanto, W. P., & Anam, M. K. (2025). Mengungkap Penggelapan Dana Nasabah: Strategi Pencegahan dan Penanganan di Era Digital. *Jurnal Ilmiah Wahana Pendidikan*, *11*(6. B), 169-181.

Sari, R. D. N. I., Istan, M., & Hendrianto, H. (2025). *Pengaruh transformasi sistem keamanan dan penggunaan teknologi baru terhadap serangan siber pada data nasabah* (Doctoral dissertation, Institut Agama Islam Negeri (IAIN) Curup).

Zahro, N., Zahra, I. A., & Faidhah, Y. S. (2024). Upaya Perlindungan Hukum Terhadap Rahasia Bank Guna Menjaga Kepentingan Nasabah Bank. *Jurnal Ilmiah Penelitian Mahasiswa*, *2*(6), 38-48.

.

.