

Reconstruction of the Integrated Online Investigation Legal Policy for Online Fraud with Victims Located Outside the Police Jurisdiction Area

Arham Gusdiar*, Ekawati, Kif Aminanto

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia; arhamgusdiar@gmail.com
Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia; ekawatikris31@gmail.com
Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia; kif.92pw@gmail.com

DOI:

<https://doi.org/10.47134/jcl.v3i3.2.6312>

*Correspondence: Arham Gusdiar

Email: arhamgusdiar@gmail.com

Received: 08/08/2026

Accepted: 27/08/2026

Published: 31/08/2026



Copyright: © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution-ShareAlike (CC BY-SA) license (<http://creativecommons.org/licenses/by-sa/4.0/>).

Abstract: The development of digital technology has led to an increase in cross-border, anonymous, and electronically based online fraud crimes, giving rise to various legal issues in the investigation process, particularly when the victim is located outside the jurisdiction of the police authority where the perpetrator committed the crime. This study aims to analyze the legal provisions governing the investigation of cross-provincial online fraud crimes within the Indonesian legal system, examine the empirical and juridical problems encountered in investigative practices, and formulate a reconstruction of an integrated online investigation legal policy based on legal certainty and digital technology. This study employs a normative legal method with a statutory and conceptual approach through an analysis of the Criminal Code (KUHP), the Criminal Procedure Code (KUHAP), the Electronic Information and Transactions Law (UU Informasi dan Transaksi Elektronik), the Law on the Indonesian National Police (Polri), and various regulations related to handling cybercrime. The results show that the applicable investigative system is still oriented towards the conventional crime paradigm and is therefore unable to accommodate the rapid, cross-border, and digital technology-based character of cybercrime. The key problems include difficulties in determining the locus delicti and tempus delicti, overlapping authority between police regions, weak

investigative coordination, limited digital forensics, slow account blocking, and poor integration of the national cyber case database. Therefore, legal policy reconstruction is needed through the establishment of an integrated cyber investigation system based on real-time investigations, strengthening cyber jurisdiction, integrating the national cyber case database, strengthening inter-agency interoperability, and legitimizing the use of artificial intelligence, cyber patrols, and digital tracking in the investigation process to create a modern, effective, and adaptive law enforcement system capable of providing legal certainty and optimal protection for victims of online fraud across provinces in Indonesia.

Keywords: integrated online investigation; online fraud; cybercrime; police jurisdiction.

Introduction

The development of digital technology in the last two decades has fundamentally changed the lifestyle of Indonesian people, especially in the fields of communication, trade, financial services, and internet-based social activities (Danuri, 2019). The growth of internet users, social media, marketplaces, mobile banking, financial technology (fintech), and digital payment systems has created a new interaction space that is virtual, fast, and cross-

border. This condition has urged increased public dependence on electronic transactions, which, on the one hand, provide efficiency and convenience, but on the other hand, give rise to increasingly complex cybercrime risks (Hapsari, R. D., & Pambayun, 2023). One of the most dominant and massive forms of cybercrime in Indonesia is online fraud carried out through social media, instant messaging applications, marketplaces, phishing, impersonation, fake investment, social engineering, and digital identity manipulation. Normatively, the online fraud can be qualified through Article 378 of the Criminal Code (KUHP), Article 28 paragraph (1) in conjunction with Article 28 paragraph (1) in conjunction with Article 378 of the Criminal Code (KUHP). Article 45A paragraph (1) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, as well as provisions regarding electronic evidence in Articles 5 and 44 of the ITE Law (Mulyadi et al., 2024). However, the development of online fraud methods has surpassed conventional criminal law constructions, as perpetrators utilize nominee accounts, virtual accounts, anonymous accounts, Virtual Private Networks (VPNs), fake digital identities, and even overseas servers to eliminate legal traces. From the perspective of Ulrich Beck's risk society theory, the modernization of digital technology has created new forms of risk that are global, abstract, and difficult to control through traditional legal instruments. Therefore, the development of online fraud crimes demonstrates that digital transformation without updates to the legal and investigative systems will create an imbalance between technological progress and the state's ability to provide legal protection to the public (Wahyudi, D., Samosir, H. S., & Devi, 2022).

The problem becomes even more complex when online fraud crimes involve victims located outside the jurisdiction of the police unit connected to the alleged perpetrator or other relevant digital infrastructure. A victim may be located in one province, while the alleged perpetrator, recipient account, electronic device, server, IP address, telecommunications data, and other electronic evidence may be connected to different regions. This situation raises a normative problem concerning the determination of *locus delicti* and *tempus delicti* because cybercrime may involve multiple legally relevant locations and digitally recorded acts rather than a single physical crime scene. The territorial principle reflected in Article 2 of the Criminal Code remains relevant, but its application requires a more adaptive jurisdictional test for electronically mediated crimes.

Therefore, this study proposes a connected cyber jurisdiction test based on four cumulative stages of assessment. First, investigators identify the location of the principal criminal conduct, namely the place from which the electronic communication, transaction, or other essential act was initiated. Second, they identify the location of the principal harmful effect, including the place where the victim suffered a direct and legally recognizable loss. Third, they identify the location of the principal evidentiary connection, particularly where the most significant electronic evidence, accounts, devices, or digital records can be lawfully secured. Fourth, they determine whether another police unit has a substantially stronger operational connection to the alleged criminal network. The *locus delicti* should therefore not be determined solely by the victim's domicile, the location of the bank account, or the location of a server. The competent investigative unit should be determined through a documented assessment of the strongest overall connection to the criminal conduct and available evidence. *Tempus delicti* should likewise be determined

through the earliest verifiable time at which an essential element of the alleged offense occurred, supported by reliable electronic timestamps, transaction records, system logs, or other authenticated digital evidence. Because this study employs a normative juridical method, the problem is formulated as a gap in the existing legal framework rather than as an independently verified empirical measurement of jurisdictional disputes (Tuju, M. C., Ramadani, S., & Nasution, 2025; Mustaqimah, 2016).

On the other hand, the weakness of legal regulations for online fraud investigations in the Indonesian legal system increasingly demonstrates the regulatory disharmony and legal gap between the development of digital crime and the prevailing criminal procedure instruments. The Criminal Procedure Code (KUHP), as the primary basis for the investigative system, is still designed based on a conventional crime paradigm oriented toward physical space, material evidence, and traditional administrative procedures. The Criminal Procedure Code (KUHP) has not yet comprehensively regulated integrated online investigation, digital case management, real-time data sharing, or a single investigation system in handling cross-regional cybercrime (Frisila, A., & Susetio, 2025). Although the ITE Law has recognized electronic evidence through Article 5 paragraph (1) and Article 44, the regulation has not yet regulated in detail the coordination mechanism for cyber investigations between regions, the governance of electronic data exchange between investigators, or the legitimacy of the use of artificial intelligence technology, cyber patrol, digital tracking, and automated investigation systems as law enforcement instruments. In addition, there is a lack of synchronization between the Criminal Procedure Code, the ITE Law, Law Number 27 of 2022 concerning Personal Data Protection, the National Police Chief Regulation concerning the investigation of cyber crimes, and the police's internal SOP regarding the management of electronic evidence (Rusmana, 2015). This state reveals that the legal substance has not been able to accommodate the dynamics of digital crime that move very quickly. From the perspective of Lawrence M. Friedman's legal system theory, the effectiveness of law enforcement is determined by the harmonization between legal substance, legal structure, and legal culture. When legal substance lags behind technological developments, the legal system loses its effectiveness in creating legal certainty and protecting the public.

This problem is increasingly relevant in the legal framework governing online fraud investigations because the applicable rules do not yet provide a sufficiently detailed and nationally integrated mechanism for determining investigative responsibility when victims, perpetrators, accounts, devices, and electronic evidence are connected to different jurisdictions. Academic literature has identified difficulties relating to jurisdictional coordination, electronic data access, digital forensic capacity, and interregional case management in the handling of cybercrime (Takanjanji, 2020). Article 43 of the ITE Law authorizes investigators to take legal measures concerning electronic systems and electronic information for law enforcement purposes. However, the existence of investigative authority does not by itself establish a comprehensive mechanism governing which police unit should lead an investigation, how related reports should be connected, or how electronic evidence should be transferred and preserved across jurisdictions. Likewise, the absence of a centralized digital investigation framework creates a normative risk of fragmented case handling and inconsistent coordination between investigative units

(Simanungkalit, J. A., Hertadi, R., & Hosnah, 2024). From the perspective of Satjipto Rahardjo's progressive legal theory, legal development must respond to changes in social and technological conditions. Therefore, the reconstruction proposed in this study focuses on strengthening the normative architecture of cyber investigation so that interregional investigations can operate through clear jurisdictional criteria, coordinated authority, and standardized digital procedures.

Based on these conditions, the need for an integrated online investigation system to address interprovincial online fraud has become increasingly urgent. A modern investigation system must be directed toward establishing a real-time coordination mechanism that enables the rapid, accurate, and integrated exchange of electronic data among investigators. Furthermore, an integrated cyber investigation system based on a unified investigative database is required to connect public reports, perpetrators' digital identities, bank accounts, electronic evidence, and digital forensic results within a single integrated national system. The model is crucial to support interoperability between law enforcement institutions, banks, fintech companies, telecommunications providers, and electronic system supervisory agencies. In this context, the concepts of smart policing, predictive policing, cyber policing, and futuristic policing are relevant as directions for modern police system reform based on digital technology. Countries such as Singapore, South Korea, the United Kingdom, Australia, and the United States have developed integrated cyber investigation systems, national cyber complaint centers, centralized cybercrime databases, and AI-based cyber investigations to handle cyber fraud. This comparison shows that Indonesia still lacks in regulatory and institutional terms in building an integrated cyber investigation system. Therefore, legal reform can no longer focus solely on adding criminal norms, but must instead be directed at reforming an effective, adaptive, and technology-based digital investigation system (Rahmad, 2019).

It is understandable that there is a serious gap between the development of online fraud crimes and the capabilities of the legal and investigative systems in Indonesia. Conventional investigation systems based on administrative jurisdiction and manual procedures are no longer capable of addressing the anonymous, transnational, rapid, and digital technology-driven nature of cybercrime. From the perspective of Gustav Radbruch's theory of legal certainty and John Rawls's theory of justice, the law must be able to provide certainty, benefit, and justice in a balanced manner to the public, including providing protection for victims of online fraud across provinces. Therefore, a reconstruction of integrated online investigation legal policies is needed, encompassing regulatory reform, institutional reform, strengthening interregional coordination, developing a national digital investigation system, and strengthening the legitimacy of technology use in the investigation process. The reconstruction is crucial for acknowledging an online fraud investigation system that is effective, transparent, accountable, adaptive to technological developments, and capable of providing legal certainty and optimal protection for victims of cybercrime across provinces in Indonesia.

Methodology

This study employs a normative juridical research method oriented towards the study of legal norms, legal principles, synchronization of laws and regulations, and legal

concepts related to integrated online investigations in handling cross-provincial online fraud crimes. The approaches used include a statutory approach and a conceptual approach. The statutory approach is carried out by examining various regulations related to the investigation system, cybercrime, police jurisdiction, electronic evidence, and law enforcement authorities, including the Criminal Code (KUHP), the Criminal Procedure Code (KUHP), Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 2 of 2002 concerning the Indonesian National Police, as well as various Regulations of the Chief of Police and regulations related to handling cybercrime. Meanwhile, a conceptual approach is used to analyze various doctrines, theories, and thoughts of legal experts related to cybercrime, cyber jurisdiction, the modern criminal justice system, integrated cyber investigation, and updates to digital technology-based investigative law. The legal materials used consist of primary, secondary, and tertiary legal materials obtained through library research. Furthermore, all legal materials are analyzed qualitatively using descriptive-analytical and prescriptive methods to identify weaknesses in the applicable legal regulations and formulate a reconstruction of integrated online investigative legal policies that are adaptive, effective, and able to provide legal certainty in handling online fraud with victims across provinces in Indonesia.

Result and Discussion

Legal Regulations for Investigation of Cross-Provincial Online Fraud Crimes in the Indonesian Legal System

The legal regulations regarding the investigation of cross-provincial online fraud crimes in the Indonesian legal system are still basically based on a combination of conventional criminal law and specific regulations in the field of information technology. Substantively, the crime of fraud is regulated in Article 378 of the Criminal Code (KUHP), which states that anyone who, with the intention of unlawfully benefiting themselves or others, uses a false name, false dignity, trickery, or a series of lies to induce others to hand over goods, grant credit, or write off receivables can be punished for fraud. In digital matters, these regulations are expanded through Article 28 paragraph (1) in conjunction with Article 45A paragraph (1) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, which regulates the prohibition on the dissemination of false and misleading news that results in consumer losses in electronic transactions. In addition, provisions regarding electronic information, electronic documents, and electronic systems are regulated in Article 1, number 1, number 2, and number 5 of the ITE Law as the legal basis for the use of digital media in transaction activities and law enforcement. Thus, online fraud is essentially a transformation of conventional fraud into cyberspace, requiring a different legal approach due to the involvement of digital technology, virtual identities, and cross-border legal relationships. However, Indonesia's positive legal regulations still demonstrate the dominance of conventional paradigms that are not fully able to address the anonymous, rapid, and unrestricted nature of cyber fraud (Sadli, 2025).

In terms of criminal procedural law, the authority to investigate online fraud is regulated in the Criminal Procedure Code (KUHAP) and the Law on the Indonesian National Police. Article 1, number 1 of the KUHAP states that investigators are officers of the Indonesian National Police or certain civil servants specifically authorized by law to conduct investigations. Furthermore, Article 6 paragraph (1) letter a of the KUHAP emphasizes that the primary investigator in criminal cases is an officer of the Indonesian National Police. The investigator's authority is more specifically regulated in Article 7 paragraph (1) of the KUHAP, which includes receiving reports, making arrests, detentions, searches, confiscations, examining documents, summoning witnesses, and terminating investigations. These regulations are reinforced through Articles 13 and 14 of Law Number 2 of 2002 concerning the Indonesian National Police, which emphasize the police's role in maintaining public security and order, law enforcement, and community protection and service. In cybercrime, investigative authority is also regulated in Article 43 of the ITE Law, which authorizes investigators within the Indonesian National Police and certain civil servants to conduct investigations into information technology crimes. However, although investigators have broad authority, the regulation does not explicitly regulate an integrated online investigation model for cross-provincial online fraud cases, thus creating coordination problems and overlapping authority between police regions (Situmorang, A. A., Neda, E. J., Rokar, I. D., & Sihotang, 2025).

Jurisdictional issues are a major problem in investigating cross-provincial online fraud crimes because the Indonesian criminal law system still relies on the principle of territoriality. Article 2 of the Criminal Code stipulates that Indonesian criminal provisions apply to anyone who commits a crime within Indonesia. This principle is essentially designed for conventional crimes that have a clearly defined locus delicti and tempus delicti. However, in cybercrime, the perpetrator, victim, server, bank account, and electronic evidence can be located simultaneously in different regions, creating difficulties in determining investigative jurisdiction. In practice, victims often report in their domicile while the perpetrator is in another province, leading to confusion regarding which police unit is authorized to handle the case. This situation is further complicated by the absence of comprehensive regulations on cyber jurisdiction in both the Criminal Procedure Code and the Electronic Information and Transactions Law. Although Article 43(6) of the Electronic Information and Transactions Law authorizes investigators to request information from electronic system providers for law enforcement purposes, there are still no detailed provisions governing cross-regional coordination or the exchange of digital evidence among investigators. As a result, there is frequent transfer of police reports between regions, duplication of case reports, and delays in case handling, which result in the loss of electronic evidence and increased losses for victims (Irawan, 2025).

In addition to jurisdictional issues, the regulation of electronic evidence in the Indonesian legal system also still faces various normative and technical limitations. Article 184 of the Criminal Procedure Code essentially only recognizes five forms of evidence: witness testimony, expert testimony, letters, clues, and defendant testimony. However, developments in digital technology have led to the recognition of electronic evidence

through Article 5 paragraphs (1) and (2) of the ITE Law, which states that electronic information and electronic documents, along with their printouts, constitute valid legal evidence and constitute an extension of the evidence recognized in Indonesian criminal procedure law (Helmawansyah, 2021). This requirement was reinforced by Constitutional Court Decision Number 20/PUU-XIV/2016, which affirms the legality of using electronic evidence as long as it is obtained legally. However, regulations regarding procedures for confiscating digital data, the chain of custody of electronic evidence, digital forensics, and the validity of cross-border electronic evidence have not been comprehensively regulated in the Criminal Procedure Code or technical police regulations (Heryogi, A., Ruba'i, M., & Sugiri, 2017). The situation creates legal uncertainty in investigative practices because each police region often has different technical standards for handling electronic evidence. Moreover, the absence of a national digital investigation system results in slow and unintegrated real-time exchange of electronic data between investigators.

Weaknesses in legal regulation are also evident in the lack of synchronization of various regulations related to handling cybercrime in Indonesia. The Criminal Procedure Code (KUHP), as general criminal procedural law, still uses an administrative and manual paradigm, while the ITE Law focuses more on the prohibition and recognition of electronic evidence without regulating the detailed governance of modern cyber investigations. Furthermore, Law Number 27 of 2022 concerning Personal Data Protection imposes certain restrictions on electronic data access, often creating a dilemma in practice between privacy protection and law enforcement interests. Likewise, various National Police Chief Regulations related to handling cybercrime, including internal regulations regarding digital forensics and cyber patrol, lack strong harmonization with the national criminal procedural law system. There are no regulations regarding integrated online investigations, a single investigation system, real-time data sharing, or interoperability between law enforcement agencies, banks, fintech companies, and telecommunications providers within a single national investigation system. Yet, the fast-moving nature of online fraud requires a technology-based investigation model and integrated electronic coordination. This lack of regulatory synchronization indicates a legal gap and legal disharmony, which has reduced the effectiveness of online fraud investigations.

Understandably, the legal framework for interprovincial online fraud investigations within the Indonesian legal system remains inadequate to address the complexities of modern digital crime. The legal system's focus on conventional crimes often hinders the investigation process due to jurisdictional issues, administrative bureaucracy, weak inter-regional coordination, and limited regulation of electronic evidence. From the perspective of Lawrence M. Friedman's legal system theory, the weak synchronization of legal substance, legal structure, and legal culture renders the law enforcement system ineffective in addressing the development of cybercrime. Therefore, legal reform is needed through the reconstruction of cyber investigation regulations that are more adaptive to developments in digital technology, including the establishment of an integrated online investigation system based on real-time coordination, strengthening cyber jurisdiction, integrating a national database of cyber cases, and strengthening the legitimacy of the use of artificial intelligence,

cyber patrols, digital tracking, and modern investigative technology in law enforcement. These reforms are crucial for achieving legal certainty, effective case handling, and optimal legal protection for victims of online fraud across provinces in Indonesia.

Problems in Investigating Online Fraud with Victims Outside Police Jurisdiction

Investigating online fraud cases with victims outside police jurisdiction presents a variety of increasingly complex legal and empirical issues with the advancement of digital technology. One key issue lies in determining the *locus delicti* and *tempus delicti* in cyberspace, which can no longer be understood conventionally as in physical crimes. In online fraud cases, the perpetrator may operate from one province, while the victim resides in another. At the same time, the bank account involved may be registered in a different region, and the server or digital platform used may be located overseas. These circumstances make it difficult to determine which police authority has jurisdiction to investigate and handle the case. Yet, the Indonesian criminal law system still bases criminal jurisdiction on the principle of territoriality as stipulated in Article 2 of the Criminal Code (KUHP). In practice, many public reports result in a tug-of-war between the district and regional police (Polda) because each region considers the *locus delicti* to be in another region. Victims are often directed to report to the region where the perpetrator's account is located or where the perpetrator is suspected of conducting electronic transactions. This situation shows that conventional criminal jurisdiction frameworks are no longer adequate to address the borderless and virtual nature of cybercrime. As a result, case handling is slowed, and victims lose access to legal certainty. This issue highlights a gap in regulations regarding cyber jurisdiction within the Indonesian criminal procedure system, particularly regarding the integrated mechanism for handling inter-provincial online fraud cases.

The next problem relates to overlapping authority and weak coordination between investigators in handling inter-regional online fraud. Normatively, Article 6 paragraph (1) and Article 7 paragraph (1) of the Criminal Procedure Code (KUHAP) grant investigators the authority of the Indonesian National Police to conduct investigations. However, the KUHAP does not provide a clear and detailed mechanism for inter-regional investigative coordination in cybercrime cases involving multiple police jurisdictions. In practice, police reports are often processed partially by different regions without a national data integration system. This results in duplication of case reports, overlapping investigations, and the potential for case termination as each region waits for transfers from other regions. Furthermore, police authorities often delay the transfer of police reports between local police stations and regional police offices because of complicated administrative procedures. These delays hinder investigators from taking swift action against perpetrators' accounts and securing electronic evidence. In addition, police units have not fully integrated their cybercrime case databases in real time, which further weakens coordination and law enforcement efforts. Many investigators in the regions still rely on manual communication through correspondence or time-consuming administrative coordination, despite the rapid and dynamic nature of online fraud. Due to this weak coordination, perpetrators often succeed in transferring criminal proceeds or erasing digital traces before the investigation process can be effectively carried out.

In addition to authority issues, serious obstacles also arise in the process of collecting and substantiating electronic evidence. Article 5 paragraphs (1) and (2) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions recognize electronic information and electronic documents as valid legal evidence. However, in investigative practice, collecting electronic evidence is not as easy as conventional evidence, requiring digital forensic skills, electronic data tracing, IP address tracking, digital data recovery, and identification of the perpetrator's electronic activity. Empirical evidence shows that digital forensic capabilities vary significantly across police jurisdictions. While some regional police departments (Polda) have adequate digital forensics laboratories, many regional police stations (Polres) lack the facilities or competent human resources for cyber investigations. Consequently, the analysis of electronic evidence often has to be delegated to the regional police or National Police headquarters, prolonging investigations. Furthermore, the lack of uniform national standards regarding the chain of custody of digital evidence often challenges the validity of electronic evidence in court proceedings. In some empirical cases, investigators have also experienced difficulties obtaining electronic data from foreign digital platforms due to jurisdictional limitations and suboptimal international cooperation in handling cybercrime.

Another major problem in inter-provincial online fraud investigations is the difficulty of blocking accounts and accessing digital financial data. Modern online fraud commonly uses nominee accounts, virtual accounts, e-wallets, and various digital payment instruments to disguise the perpetrator's identity. Normatively, Article 43 paragraphs (3) and (5) of the ITE Law authorize investigators to take legal action against electronic systems and obtain electronic information for law enforcement purposes. However, in practice, the account blocking process is often hampered by bureaucratic hurdles between agencies, slow responses from banking institutions, and violations of customer data confidentiality provisions as stipulated in the Banking Law. Many cases indicate that proceeds of crime have been transferred or withdrawn before the blocking process is complete. Furthermore, coordination between investigators and fintech operators, marketplaces, telecommunications providers, and social media platforms has not been optimal. Investigators often encounter administrative obstacles in requesting user data, electronic transaction history, and the perpetrator's digital identity data. However, the speed of electronic data access is crucial for successfully uncovering online fraud cases. Poor system integration between agencies results in slow, ineffective investigations, and often loses momentum in enforcing the law against cyber fraud perpetrators.

In addition to structural and technical barriers, the quality of human resources for cyber investigators in the regions is also a serious issue in handling interprovincial online fraud. The rapid development of cybercrime methods requires investigators with expertise in information technology, digital intelligence, cyber patrol, open source intelligence, and digital forensics. However, empirical evidence shows that not all police regions have investigators with specialized cyber competencies. Many investigators still use conventional investigative approaches to digital cases, resulting in suboptimal investigations. Limited training, minimal investigative technology budgets, and uneven distribution of cyber

laboratories contribute to differences in the capacity to handle cybercrime cases across regions. Furthermore, in public reporting practices, the phenomenon of victim blaming still occurs, especially for online fraud victims who are perceived as being careless in conducting electronic transactions. This situation demonstrates the weak perspective on victim protection within Indonesia's cyber law enforcement system. Consequently, many victims are reluctant to pursue legal proceedings because they feel they lack protection and certainty of case resolution. The low resolution rate of online fraud cases ultimately impacts public trust in law enforcement institutions.

These various problems indicate that the investigation system for online fraud across provinces in Indonesia still faces serious challenges in regulations, institutions, technology, and human resources. The criminal procedure system, which is still oriented towards conventional crimes, makes handling cybercrime ineffective in dealing with the anonymous, rapid, and transnational nature of digital crime. From the perspective of Lawrence M. Friedman's legal system theory, the weak synchronization between legal substance, legal structure, and legal culture causes the law enforcement system to be unable to function optimally. Furthermore, from the perspective of Satjipto Rahardjo's progressive legal theory, the law should evolve to follow the needs of society and technological developments, so that bureaucratic and formalistic investigative approaches are no longer adequate in dealing with modern cybercrime. Therefore, the empirical and legal problems in investigating online fraud across provinces demonstrate the urgency of establishing an integrated online investigation system based on digital technology, strengthening coordination between police regions, integrating the national cyber case database, accelerating access to electronic data across institutions, and strengthening the capacity of cyber investigators to achieve legal certainty and effective victim protection in Indonesia.

Reconstruction of Integrated Online Investigation Legal Policy in Handling Cross-Provincial Online Fraud Based on Legal Certainty and Digital Technology

The development of interprovincial online fraud requires a reconstruction of investigative legal policies that are no longer oriented solely to conventional patterns based on administrative jurisdiction, but rather directed towards an integrated online investigation model based on digital technology. This reconstruction must begin with updating the legal substance through reformulation of the Criminal Procedure Code (KUHP), the Electronic Information and Transactions Law, and internal police regulations to accommodate the borderless, real-time, and digital nature of cybercrime. Specifically, new legal norms are needed that explicitly regulate integrated cyber investigation systems, cyber jurisdiction, digital evidence management, and real-time interregional investigation within the national investigation system. These regulations must provide legal legitimacy for the use of artificial intelligence, cyber patrol, digital tracking, open-source intelligence, and automated tracing systems as official instruments for investigating cybercrime. Furthermore, it is necessary to establish specific Government Regulations and National Police Chief Regulations concerning mechanisms for handling interprovincial online fraud that regulate national digital reporting procedures, interregional electronic data exchange, rapid account blocking management, and nationally applicable digital forensics operational

standards. This regulatory reform is crucial to address the legal disharmony between the Criminal Procedure Code (KUHP), Law Number 1 of 2024 concerning Electronic Information and Transactions, Law Number 27 of 2022 concerning Personal Data Protection, and other sectoral regulations that have been partially implemented in handling cybercrime.

The next reform should focus on developing an integrated online investigation system that enables real-time coordination among police work units through a single National Integrated Cyber Investigation Platform. The Platform should connect Polres, Polda, and Mabes Polri through an integrated digital system and may contain legally relevant identifiers, including suspect-related identities where available, account numbers, telephone numbers, social-media accounts, IP addresses, transaction patterns, and victim report histories. However, the collection and processing of such information must comply with the principles of legality, purpose limitation, data minimization, necessity, proportionality, security, and accountability as reflected in Law Number 27 of 2022 concerning Personal Data Protection.

Access should therefore be based on a role-based access control system, under which investigators may only access data necessary for their assigned case. Highly sensitive data should be protected through encryption, strong authentication, access logging, periodic security testing, and an auditable record of every access, modification, transfer, and disclosure. Data retention periods should be differentiated according to whether information remains necessary for an active investigation, evidentiary preservation, judicial proceedings, or legally required archival purposes. Unauthorized access, disclosure, alteration, or use of data outside an authorized investigative purpose should result in administrative, disciplinary, and, where applicable, criminal consequences.

The system should not automatically merge reports merely because they contain similar account numbers, telephone numbers, names, or transaction patterns. Instead, the Platform should conduct case-linkage analysis based on multiple indicators, including common digital identifiers, transaction patterns, modus operandi, temporal proximity, device or IP relationships, and other legally relevant connections. An automated system may generate a linkage recommendation, but the decision to merge reports or establish a joint investigation must remain subject to human verification by an authorized investigator. Reports that are not sufficiently connected should remain separate. This mechanism would reduce duplication and overlapping investigations without creating the risk of prematurely combining unrelated cases.

In addition to strengthening the digital system, legal policy reconstruction must also be directed at reformulating cross-jurisdictional investigative authority in online fraud cases. The concept of connected jurisdiction or cyber jurisdiction should not mean that every police unit connected to a digital offense has equal authority to conduct a separate investigation. Instead, connected jurisdiction should function as a legal basis for identifying one lead investigative unit while allowing other police units to provide coordinated operational assistance. The designation of the lead investigative unit should follow a structured priority test based on: first, the location of the principal criminal conduct; second, the location with the strongest concentration of relevant electronic or physical evidence;

third, the scale and geographical spread of the suspected criminal network; and fourth, the operational capacity required to handle the case.

At the initial reporting stage, a Polres may receive a victim's report regardless of the eventual location of the alleged perpetrator. The report should then be entered into the national platform and subjected to a jurisdictional assessment. Cases with a predominantly local connection may remain under Polres coordination; cases involving multiple districts within one province may be coordinated by the relevant Polda; while cases involving multiple provinces, organized digital networks, significant national impact, or complex technological infrastructure may be coordinated by the national cyber unit at Mabes Polri. Where more than one unit has a substantial connection, the National Integrated Cyber Investigation Platform should record the competing connections and designate a lead unit through a documented coordination decision. Other units should act as assisting investigators rather than opening parallel investigations unless new and materially distinct criminal conduct is identified. A national cyber investigation coordination center may supervise this allocation of authority and resolve jurisdictional disputes. In this manner, cyber jurisdiction becomes a mechanism for allocating authority rather than multiplying authority.

Legal policy reconstruction must also include strengthening interoperability between law enforcement agencies, banks, fintech companies, telecommunications providers, marketplaces, and electronic system providers through a legally regulated cybercrime response network. Such interoperability should not create unrestricted access to customer or user data. Instead, investigative requests should be processed through an Electronic Legal Request Gateway that records the identity of the requesting investigator, legal basis, case number, category of requested data, purpose of the request, authorization status, date and time of submission, and the responding institution. Access to personal data should be limited to information that is necessary and proportionate to a specific lawful investigation and must remain consistent with Law Number 27 of 2022 concerning Personal Data Protection and applicable sectoral confidentiality obligations.

National regulations should establish differentiated response-time standards based on the urgency and category of the request. Emergency preservation requests involving an immediate risk that criminal proceeds or electronic evidence will disappear should receive an initial response through an expedited mechanism, while ordinary investigative requests should be processed within a predetermined statutory or regulatory time limit. The exact response periods should be determined by regulation according to the nature of the data and operational capacity of each sector. Failure to comply without lawful justification should be subject to administrative sanctions and supervisory review.

A temporary emergency account freeze should only be permitted where there are documented reasonable grounds supported by at least identifiable transaction records, victim reports, or other preliminary electronic evidence indicating a substantial connection between the account and an alleged online fraud offense. The request should be authorized by a designated senior investigative officer and electronically recorded through the national platform. Emergency freezing should be temporary and limited in duration, subject to

prompt review by the competent authority under procedures established by law. The account holder must be provided with an accessible mechanism to challenge the freeze, submit evidence of legitimate ownership or transactions, and obtain restoration or compensation where a blocking measure is found to have been unlawful or unjustified. Any extension of the freeze should require a renewed evidentiary assessment and formal authorization. Thus, rapid action against suspected criminal proceeds can be balanced with legal protection for legitimate account holders.

In terms of criminal evidence, legal policy reform needs to be directed at strengthening the legitimacy of electronic evidence and standardizing digital forensics nationally. Article 5, paragraphs (1) and (2) of the Electronic Information and Transactions Law recognize electronic evidence as valid legal evidence, but technical regulations regarding the chain of custody, digital evidence preservation, forensic acquisition, and cross-border electronic evidence remain very limited. Therefore, the establishment of national standards for digital evidence handling that apply uniformly to all law enforcement officers in Indonesia is necessary. Specifically, the Indonesian National Police (Polri) needs to establish regional digital forensics laboratories in each regional police station, integrated with the national cybercrime data center. Furthermore, investigators must receive specialized training in cyber investigation, artificial intelligence investigation, blockchain tracing, cryptocurrency tracking, and advanced digital forensics regularly. The government also must assemble international collaboration with global digital platforms and foreign law enforcement agencies to facilitate the exchange of electronic evidence across borders. This capacity building is crucial to ensure that digital evidence has strong legal validity and can be used effectively in the process of proving cross-border online fraud.

The reconstruction of integrated online investigative legal policy must be directed toward the establishment of a modern, adaptive, transparent cyber law enforcement system oriented toward legal certainty and victim protection. From the perspective of Satjipto Rahardjo's progressive legal theory, law must adapt to social and technological developments. Therefore, the government should establish a National Cyber Complaint Center through a national digital reporting application that enables victims to submit online fraud reports regardless of their geographical location. The system should automatically generate a unique report number and conduct an initial case-linkage assessment without preventing the victim from maintaining an independent report where the connection with another case has not yet been verified.

The reporting system should provide victims with controlled access to procedural information concerning the registration of the report, the responsible investigative unit, the general stage of case handling, requests for additional information, and decisions that directly affect the status of the report. However, access should not extend to confidential investigative strategies, the personal data of other victims or suspects, protected witness information, unverified allegations, or other information whose disclosure could compromise an ongoing investigation or the rights of third parties. The Platform should therefore distinguish between an investigative workspace accessible only to authorized officials and a victim case-progress interface containing limited procedural information.

The National Cyber Complaint Center should also operate under clear accountability mechanisms, including complaint procedures for delayed handling, access logs for officials, periodic system audits, and internal or external review of alleged misuse of investigative data. In this manner, digital transparency can improve victim access and institutional accountability without compromising personal-data protection, investigative integrity, or due process.

To provide a concrete normative direction, the proposed reconstruction should be translated into specific amendments to the Criminal Procedure Code, the Electronic Information and Transactions Law, and relevant National Police regulations. First, the Criminal Procedure Code should contain a provision on cyber jurisdiction establishing a connected jurisdiction test and a mandatory mechanism for designating one lead investigative unit in interregional cyber cases. Second, national digital reporting should permit victims to submit reports irrespective of their domicile while requiring immediate registration and jurisdictional assessment through the National Integrated Cyber Investigation Platform. Third, interregional investigative authority should regulate the division between lead investigators and assisting investigators and provide a formal procedure for resolving jurisdictional disputes. Fourth, emergency account freezing should require documented reasonable grounds, authorized approval, limited duration, periodic review, and a remedy mechanism for wrongful blocking. Fifth, digital evidence provisions should establish national chain-of-custody standards, integrity verification, secure transfer, and documentation requirements. Sixth, AI-assisted investigation should be limited by standards of validation, explainability, human oversight, bias assessment, auditability, and evidentiary verification. Seventh, the relevant police regulations should establish mandatory interoperability procedures and response standards for lawful investigative requests to financial institutions, telecommunications providers, marketplaces, and electronic system operators. Finally, the framework should guarantee victims access to limited case-progress information and provide administrative, disciplinary, or other applicable sanctions for unauthorized data disclosure, manipulation of digital evidence, unlawful access, failure to comply with lawful interoperability obligations, or misuse of AI-assisted investigative systems.

Conclusion

Based on the discussion, it can be concluded that the legal regulations for investigating online fraud across provinces in Indonesia essentially have a normative basis through the Criminal Code (KUHP), the Criminal Procedure Code (KUHAP), Law Number 1 of 2024 concerning Electronic Information and Transactions, and Law Number 2 of 2002 concerning the Indonesian National Police. However, the existing legal construction is still oriented towards the conventional crime paradigm and therefore unable to address the complexity of cybercrime, which is anonymous, fast, cross-regional, and digital technology-based. Empirical problems indicate difficulties in determining the locus delicti and tempus delicti in cyberspace, overlapping authority between police regions, weak coordination between investigators, limited digital forensics, slow account blocking, low integration of cyber case

databases, and suboptimal access to electronic data from banks, fintech, and digital providers. This situation is further worsened by regulatory inconsistencies, the absence of clear norms governing integrated cyber investigations, and the lack of a nationally integrated, real-time digital investigation system. Therefore, a reconstruction of integrated online investigation legal policy is necessary through regulatory reformulation, strengthening cyber jurisdiction, establishing a single investigation system, integrating a national cyber case database, strengthening inter-agency interoperability, and legitimizing the use of artificial intelligence, cyber patrol, and digital tracking in the investigation process to ensure legal certainty and optimal protection for victims of online fraud across provinces in Indonesia.

In this regard, it is suggested that the government and legislative institutions immediately update the Criminal Procedure Code (KUHP) and regulations related to cybercrime by incorporating specific provisions regarding integrated online investigations, cyber jurisdiction, real-time investigation systems, and comprehensive management of electronic evidence and digital forensics. Furthermore, the Indonesian National Police (Polri) needs to establish a National Integrated Cyber Investigation Platform that is connected nationally from the police precinct (Polres), regional police (Polda), to the National Police Headquarters (Mabes Polri) through a digital investigation system based on artificial intelligence and one data investigation. The government also needs to strengthen coordination between law enforcement agencies, banks, fintech companies, telecommunications providers, and electronic system operators by establishing an integrated cybercrime response network to expedite account blocking, electronic data access, and digital evidence tracking. Furthermore, continuous capacity building for cyber investigators through education in digital forensics, cyber intelligence, and advanced cyber investigation is essential to ensure law enforcement is able to keep pace with increasingly complex digital crime modes. With regulatory updates, institutional strengthening, integration of investigative technology, and a modern and adaptive national coordination system, it is hoped that handling of online fraud across provinces in Indonesia will be more effective, transparent, and accountable, and able to provide justice and legal certainty for the public in the era of digital transformation.

References

- Danuri, M. (2019). Perkembangan dan Transformasi Teknologi Digital. *Jurnal Ilmiah Infokam*.
- Frisila, A., & Susetio, W. (2025). Perlindungan Hukum Atas Penipuan Online dengan Modus Pekerjaan Freelance Melalui Media Sosial Ditinjau dari KUHP dan UU ITE. *Arus Jurnal Sosial Dan Humaniora*, 2124–2134.
- Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman Cybercrime di Indonesia: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*, 1–17.
- Helmawansyah, M. (2021). Penggunaan Barang Bukti Elektronik yang Dijadikan Alat Bukti dalam Perkara Pidana. *Journal of Law (Jurnal Ilmu Hukum)*, 6(1), 527–541.
- Heryogi, A., Ruba'i, M., & Sugiri, B. (2017). Fungsi Bukti Elektronik Dalam Hukum Acara Pidana Pasca Putusan Mahkamah Konstitusi Nomor 20/Puu-Xiv/2016. . . *Jurnal Ilmiah Pendidikan Pancasila Dan Kewarganegaraan*, 7–17.

- Irawan, D. (2025). Tinjauan Yuridis terhadap Tindak Pidana Siber. *Jurnal Litbang Polri*, 138–152.
- Mulyadi, Nurdin, A. A., Anjani, A. A., Alamsyah, F. D., Sifana, F., Yudistio, M. A., Maulana Muhammad Kareem, & Rabbani, R. A. A. (2024). Media Hukum Indonesia (MHI) Analisis Penipuan Online Melalui Media Sosial Dalam Perspektif Kriminologi. *Media Hukum Indonesia (MHI)*, 2(2), 74. <https://doi.org/10.5281/zenodo.11183088>
- Mustaqimah, L. (2016). Penerapan Asas Nasionalitas Pasif Terhadap Tindak Pidana Teknologi Informasi. *Badamai Law Journal*, 322–342.
- Rahmad, R. A. (2019). Hukum Acara Pidana Ω. In *Hukum Acara Pidana* (Vol. 6, Number 2). Sinar Grafika.
- Rusmana, A. (2015). Penipuan dalam Interaksi melalui Media Sosial (Kasus Peristiwa Penipuan melalui Media Sosial dalam Masyarakat Berjejaring). *Jurnal Kajian Informasi Dan Perpustakaan*, 187–194.
- Sadli, D. C. (2025). Implementasi Undang-Undang Informasi dan Transaksi Elektronik terhadap Kasus Penipuan Online di Provinsi Lampung. *Jurnal Hukum Lex Generalis*.
- Simanungkalit, J. A., Hertadi, R., & Hosnah, A. U. (2024). Analisis Tindak Pidana Penipuan Online dalam Konteks Hukum Pidana Cara Menanggulangi dan Pencegahannya. *AKADEMIK: Jurnal Mahasiswa Humanis*, 281–294.
- Situmorang, A. A., Neda, E. J., Rokar, I. D., & Sihotang, R. S. (2025). Analisis Penegakan Hukum Terhadap Penyidikan Penipuan Online di Wilayah Hukum Polres Bangka. *Iuris Studia: Jurnal Kajian Hukum*, 632–641.
- Takanjanji, J. (2020). Merefleksi Penegakan Hukum Tindak Pidana Penipuan Online. *Widya Pranata Hukum: Jurnal Kajian Dan Penelitian Hukum*, 75–90.
- Tuju, M. C., Ramadani, S., & Nasution, C. (2025). Penegakan Hukum Terhadap Tindak Pidana Cyber dalam Kasus Penipuan Jual Beli Online dalam Perspektif Kriminologi. *Innovative: Journal of Social Science Research*, 1763–1776.
- Wahyudi, D., Samosir, H. S., & Devi, R. S. (2022). Akibat Hukum bagi Pelaku Tindak Pidana Penipuan Online melalui Modus Arisan Online di Media Sosial Elektronik. *JURNAL RECTUM: Tinjauan Yuridis Penanganan Tindak Pidana*, 326–336.