Customary Law Journal, AICOPS Special Collection 2026, *Page*: 1-14

Reconstruction of the Police Intelligence Legal System to Address the Failure of Decision-Making in Detecting Transnational Crimes in a Just and Legally Certain Way

Giovanni Ruben Siregar*, Yopik Gani, Kif Aminanto

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia; giovanniruben611@gmail.com
Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia; yopikgadi@gmail.com
Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia; kif.92pw@gmail.com

DOI:
https://doi.org/10.47134/jcl.v3i3.2.6306
*Correspondence: Giovanni Ruben Siregar
Email: giovanniruben611@gmail.com

Received: 08/08/2026
Accepted: 24/08/2026
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: *This study seeks to examine weaknesses in the police intelligence legal framework in detecting and making decisions related to transnational crimes, as well as to reconstruct the system by introducing predictive policing and an integrated criminal intelligence approach that ensures fairness and legal certainty. The research employs a normative juridical method with statutory and conceptual approaches, analyzing the 1945 Constitution of the Republic of Indonesia, Law Number 2 of 2002 on the Indonesian National Police, Law Number 17 of 2011 on State Intelligence, and other relevant regulations concerning transnational crime and police intelligence. The findings show that the shortcomings of police intelligence in addressing transnational crime stem from regulatory inconsistencies, weak integration of intelligence data, limited inter-agency coordination, unclear decision-making procedures, and insufficient oversight and human rights safeguards. These conditions indicate that conventional law enforcement methods are increasingly inadequate in responding to transnational crimes that are cross-border, organized, and technologically advanced. This research proposes a reconstruction of the police intelligence legal system through regulatory reform, the development of an integrated criminal intelligence system, the strengthening of predictive policing based on artificial intelligence and big data analytics, the establishment of an independent oversight mechanism, and the strengthening of international cooperation to create a modern, preventative, predictive, accountable, and equitable police intelligence system for combating transnational crime.*

Keywords: *Police Intelligence, Predictive Policing, Transnational Crime.*

Introduction

The development of globalization and digitalization has given rise to a major transformation in modern crime patterns that are no longer limited by the territorial jurisdiction of a country. The phenomenon of borderless crime has caused crime to become increasingly complex, organized, and high-tech-based, thus surpassing the capabilities of conventional law enforcement, which has been repressive and reactive (Insani et al., 2026). Transnational crime currently includes not only international narcotics trafficking, human trafficking, cybercrime, terrorism financing, arms smuggling, and cross-border money laundering, but has also utilized anonymous networks, crypto currencies, the dark web, artificial intelligence, and encrypted communication systems that complicate the process of detection and legal evidence (Naseh, 2019). This condition shows that transnational crime

has developed into an extraordinary crime that threatens national stability, state security, the rule of law, the protection of human rights, and national economic resilience. Normatively, regulations on transnational crime have obtained international legitimacy through the United Nations Office on Drugs and Crime and the 2000 Palermo Convention, or the United Nations Convention against Transnational Organized Crime, which underscores the obligation of states to strengthen cross-border intelligence and law enforcement cooperation (Tabiu et al., 2023). At the national level, Article 30, paragraph (4) of the 1945 Constitution of the Republic of Indonesia affirms that the Indonesian National Police is tasked with protecting, serving, and enforcing the law. This provision is further elaborated in Article 13 of Law Number 2 of 2002 concerning the Indonesian National Police, which places the maintenance of public security and order and law enforcement as the primary functions of the police (Arif, 2021). However, the increasingly sophisticated development of transnational crime demonstrates that conventional law enforcement approaches relying on post-crime repressive measures are no longer adequate, necessitating a transformation of the police intelligence system based on early detection, predictive analysis, and strategic decision-making.

In the modern law enforcement system, police intelligence has a very strategic position as an early warning system, strategic detection, and preventive policing in preventing the development of transnational crime threats. Police intelligence is no longer understood only as an information-gathering instrument, but as a security analysis system that functions to identify threats, map criminal networks, predict risks, and prepare recommendations for strategic decision-making for law enforcement officers (Husen et al., 2020). This function is in line with Article 14 paragraph (1) letter g of Law Number 2 of 2002, which gives the National Police the authority to conduct investigations and inquiries into all criminal acts in accordance with criminal procedure law and other laws and regulations, which, in practice, are highly dependent on the quality of the intelligence system. In addition, Article 6 of Law Number 17 of 2011 concerning State Intelligence emphasizes that state intelligence has the functions of investigation, security, and mobilization for the interests of national security (Ismail, 2023). In modern policing, intelligence-led and predictive policing have emerged as a paradigm that prioritizes intelligence as the foundation for operational decision-making. This approach allows the police to detect crime patterns, identify transnational actors, and anticipate risks before they materialize. Consequently, the effectiveness of law enforcement decisions depends heavily on the quality of the intelligence system, as failures in intelligence can directly compromise the state's ability to protect the public from the increasingly complex and adaptive threats posed by transnational crime (Pramawi Nicolas Huliselan, 2023).

The strategic importance of police intelligence does not necessarily mean that every continuing occurrence of transnational crime can automatically be characterized as an empirical failure of intelligence institutions. Rather, from a normative juridical perspective, the persistence and increasing complexity of international narcotics trafficking, human trafficking, transnational cybercrime, terrorist financing, and cross-border money laundering demonstrate the continuing need to evaluate whether the existing legal framework provides sufficiently clear authority, coordination mechanisms, analytical standards, and accountability procedures for early detection and strategic decision-making.

Various reports and studies concerning transnational crime have also highlighted persistent problems relating to weak coordination between countries, fragmented information exchange, and limited integration of intelligence data (Harefa, 2018). In practice, these conditions may result in information overload, fragmentation between agencies, weak risk analysis, limited database interoperability, and delayed strategic responses. Therefore, the problem examined in this study is not intended to establish empirically that particular intelligence officers or institutions have failed in specific cases, but rather to identify normative and institutional vulnerabilities within the Indonesian police intelligence legal system that may affect the effectiveness of early detection and decision-making in responding to transnational crime (Seh et al., 2020).

This problem is further complicated by the fragmented legal framework governing police intelligence and intelligence-related decision-making in Indonesia. Relevant authority is distributed across Law Number 2 of 2002 concerning the Indonesian National Police, Law Number 17 of 2011 concerning State Intelligence, the Criminal Procedure Code, Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law, Law Number 35 of 2009 concerning Narcotics, and other sectoral regulations. The normative problem does not merely arise from the existence of multiple regulations, but from the absence of sufficiently clear legal connections between them. Law Number 2 of 2002 regulates the authority of the Indonesian National Police to conduct inquiries and investigations, while Law Number 17 of 2011 regulates intelligence functions relating to investigation, security, and mobilization for national security. However, the relationship between intelligence analysis, operational decision-making, preliminary inquiry, investigation, and the subsequent use of information in criminal proceedings remains insufficiently defined. Similarly, although Article 43 of Law Number 17 of 2011 requires coordination and information sharing among intelligence agencies, the law does not establish detailed standards concerning data interoperability, institutional access, responsibility for inaccurate information, or the legal consequences of automated intelligence analysis. Article 31 of the same law also recognizes intelligence activities such as interception in accordance with statutory provisions, yet the legal framework does not comprehensively regulate a uniform threshold, authorization procedure, duration, renewal mechanism, emergency exception, or independent review applicable to intrusive intelligence measures (Wirandy & Syaufi, 2025). These normative gaps create uncertainty concerning the limits of authority, the legality of intelligence-based decision-making, the protection of personal data, and the accountability of intelligence actions that may restrict citizens' rights.

This situation demonstrates a gap between the normative expectation that police intelligence should operate accurately, rapidly, in an integrated manner, and accountably, and the existing legal framework, which has not yet comprehensively regulated the transition from conventional intelligence practices to technology-assisted predictive analysis. The Indonesian legal framework recognizes intelligence activities and information-based policing, but it does not yet provide a specific legal architecture governing predictive policing, artificial intelligence-assisted analysis, automated risk assessment, algorithmic accountability, or the interoperability of criminal intelligence data. Consequently, the legal issue is not simply whether intelligence information can be

collected, but how information may be processed, integrated, analyzed, retained, and transformed into lawful strategic decisions. This distinction is particularly important because intelligence-led policing and predictive policing should not be treated as identical concepts. Intelligence-led policing provides a broader institutional and decision-making framework in which intelligence supports policing priorities, whereas predictive policing constitutes a more specific analytical approach that uses historical and real-time data, pattern recognition, and risk assessment to anticipate potential criminal threats. Therefore, predictive policing should be legally positioned as a technologically enhanced analytical component within a broader intelligence-led policing framework, rather than as a replacement for human intelligence analysis or an autonomous decision-making system.

Based on these issues, the reconstruction of the police intelligence legal system should not merely introduce new technologies into existing intelligence practices, but should establish a legally bounded framework for predictive and integrated criminal intelligence. Such reconstruction should include regulatory harmonization, clear functional boundaries between intelligence and investigation, standards for the interoperability of criminal intelligence data, and explicit legal requirements governing the collection, processing, storage, retention, access, and use of personal data in artificial intelligence-assisted intelligence systems. The proposed framework must also ensure that automated analysis cannot independently determine coercive measures against individuals. Artificial intelligence and automated risk assessment may assist in identifying patterns, generating risk indicators, and supporting analytical recommendations, but the final decision concerning surveillance, investigation, or other measures affecting individual rights must remain subject to meaningful human evaluation. The reconstruction should further establish algorithmic audit mechanisms, bias testing, documentation requirements, independent oversight, judicial control over intrusive intelligence measures, and clear procedural boundaries between intelligence information and admissible criminal evidence. In this manner, the proposed reconstruction is directed not only toward improving the effectiveness of detecting transnational crimes but also toward ensuring that technology-assisted intelligence remains compatible with legal certainty, accountability, due process of law, proportionality, and human rights protection as guaranteed in Article 28D paragraph (1) and Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia.

Methodology

This research employs a normative juridical legal research method that focuses on the study of norms, principles, theories, and legal systems related to police intelligence in combating transnational crime. The approaches used include a statutory approach and a conceptual approach. The statutory approach is carried out by examining various relevant legal provisions, including the 1945 Constitution of the Republic of Indonesia, Law Number 2 of 2002 concerning the Indonesian National Police, Law Number 17 of 2011 concerning State Intelligence, the Criminal Procedure Code, Law Number 1 of 2024 concerning Electronic Information and Transactions, Law Number 35 of 2009 concerning Narcotics, as well as various international legal instruments related to transnational crime and international intelligence cooperation. Meanwhile, a conceptual approach is used to analyze the concept of the rule of law, intelligence-led policing, predictive policing, intelligence

decision-making systems, legal certainty, justice, human rights protection, and modern law enforcement theories that have developed in legal doctrine and literature. The legal materials used consist of primary, secondary, and tertiary legal materials obtained through library studies and analyzed prescriptively and analytically using legal interpretation techniques, legal argumentation, and deductive reasoning to find normative weaknesses in the police intelligence legal system and formulate an ideal, adaptive, and just legal reconstruction model in facing the complexity of modern transnational crime.

Result and Discussion

Weaknesses of the Police Intelligence Legal System in Detecting and Decision-Making on Transnational Crimes

The police intelligence legal system is essentially an integral part of the national security and law enforcement framework, which has a strategic function in detecting, analyzing, and responding to the threat of transnational crime. From the perspective of a state based on law, as stated in Article 1 paragraph (3) of the 1945 Constitution of the Republic of Indonesia, all police intelligence activities must be carried out based on the principles of legality, accountability, proportionality, and protection of human rights. The position of the Indonesian National Police as a law enforcement institution is regulated in Article 30 paragraph (4) of the 1945 Constitution of the Republic of Indonesia and further elaborated in Article 13 of Law Number 2 of 2002 concerning the Indonesian National Police. In the context of transnational crime, intelligence therefore functions as an instrument for early detection, threat assessment, strategic analysis, and decision support. However, the normative vulnerability of the existing system lies in the fact that these functions are regulated through multiple legal instruments without a sufficiently integrated framework defining the relationship between intelligence collection, intelligence analysis, policing decisions, preliminary inquiry, criminal investigation, and the evidentiary process. As a result, the legal issue examined in this study concerns the adequacy of the existing legal architecture in supporting modern intelligence functions rather than establishing empirical responsibility for particular intelligence failures (Ubaidillah et al., 2025).

The first normative weakness lies in the insufficiently defined relationship among legal provisions governing police authority, state intelligence functions, criminal procedure, and sectoral crime prevention. Law Number 17 of 2011 regulates the functions of state intelligence, including investigation, security, and mobilization for national security, while Law Number 2 of 2002 authorizes the Indonesian National Police to conduct inquiries and investigations into criminal acts. The problem is not necessarily a direct contradiction between these provisions, but the absence of a detailed legal framework distinguishing intelligence analysis from criminal inquiry and investigation, particularly when intelligence information becomes the basis for operational or strategic law-enforcement decisions. This uncertainty is further connected with the Criminal Procedure Code, which regulates the formal evidentiary process but does not comprehensively define the legal transition from intelligence information into information obtained through lawful investigative procedures. Likewise, Article 43 of Law Number 17 of 2011 requires coordination and intelligence

information sharing, but does not establish detailed standards concerning interoperability, access authorization, data quality, responsibility, retention, or auditability. Regulations concerning electronic information and sectoral crimes provide additional authority regarding digital information and specific criminal threats, yet they do not collectively establish a unified framework for AI-assisted intelligence analysis, automated risk classification, or predictive policing. Consequently, the normative gap is located in the absence of clear legal boundaries and procedural connections between intelligence authority, investigative authority, data processing, technology-assisted analysis, and criminal procedural safeguards (Wulandari & Tofan, 2026).

In addition to these regulatory gaps, the weakness of the police intelligence legal system is also evident in the absence of comprehensive standards governing intelligence-based decision-making. Existing legal provisions recognize intelligence functions and police authority, but do not specifically establish a structured process for determining how intelligence should be assessed before it becomes the basis for strategic or operational decisions. In the context of modern transnational crime, such a process should include the verification of data sources, reliability assessment, threat classification, proportionality analysis, documentation of analytical reasoning, and human responsibility for the final decision. The absence of such standards becomes increasingly significant when intelligence analysis is assisted by artificial intelligence, big data analytics, facial recognition, or automated risk assessment. These technologies may improve the capacity to identify patterns and connections that cannot easily be detected through conventional analysis, but they may also generate false positives, inaccurate classifications, discriminatory profiling, and algorithmic bias. Therefore, predictive analysis should not be understood as an automated decision-making mechanism. Any AI-generated output must function as an analytical recommendation subject to human review, and no coercive or rights-restricting action should be based solely on an automated risk classification. The legal framework should consequently require prior validation, periodic accuracy testing, bias assessment, documentation of algorithmic inputs and outputs, and an auditable record of the human decision-maker responsible for acting upon intelligence analysis (Debora et al., 2025).

The next weakness relates to the low level of integration of intelligence information systems and the weak coordination between law enforcement agencies. To combat transnational crime, police intelligence requires a fast, accurate, and integrated information exchange system, both nationally and internationally. However, the reality is that intelligence data is still scattered across various institutions, such as the Indonesian National Police (Polri), the National Narcotics Agency (BNN), the Financial Transaction Reports and Analysis Center (PPATK), the Directorate General of Immigration, and other security agencies, without optimal interoperability mechanisms. This situation leads to information fragmentation and hinders comprehensive threat analysis. This is despite Article 43 of Law Number 17 of 2011 stating that state intelligence officials are required to coordinate and share intelligence information for the benefit of national security. Furthermore, provisions in the 2000 United Nations Convention against Transnational Organized Crime, ratified by Indonesia through Law Number 5 of 2009, also emphasize the importance of international

cooperation and information exchange in combating transnational organized crime. Weak database integration and coordination between agencies often result in law enforcement officials failing to detect transnational network patterns early, resulting in slow, reactive, and ineffective crime handling (Pohan, 2025).

Another crucial issue is the weak oversight and accountability system for the use of police intelligence powers. In a democratic state governed by the rule of law, the use of intelligence powers must be subject to the principle of checks and balances to prevent abuse of power and human rights violations. However, intelligence regulations in Indonesia still lack oversight mechanisms, judicial control, and independent audits of police intelligence activities. Article 31 of Law Number 17 of 2011 grants state intelligence the authority to wiretap based on statutory regulations, but it is not accompanied by detailed regulations regarding limitations, oversight mechanisms, or protection of citizens' privacy rights. This situation has the potential to lead to abuse of power, unlawful surveillance, and arbitrary use of intelligence data, which violates Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which guarantees the protection of the privacy, honor, dignity, and security of citizens. Furthermore, Article 28D paragraph (1) of the 1945 Constitution affirms the right of every person to recognition, guarantees, protection, and fair legal certainty (Sirait & Abdillah, 2025). Thus, weak oversight of police intelligence not only impacts the effectiveness of law enforcement but also has the potential to violate the principle of due process of law and citizens' constitutional rights.

Based on these weaknesses, the Indonesian police intelligence legal system faces fundamental normative issues concerning the relationship between intelligence and investigation, the integration of information, the use of technology-assisted analysis, the accountability of decision-making, and the protection of constitutional rights. The central problem is therefore not merely the absence of technological capacity, but the absence of a sufficiently integrated legal framework determining how intelligence data may be collected, processed, analyzed, shared, retained, audited, and used as a basis for strategic decisions. Intelligence information should remain distinguishable from criminal evidence. Intelligence may identify threats, map criminal networks, generate investigative leads, and support the prioritization of law-enforcement activities, but intelligence information should not automatically be treated as admissible evidence in criminal proceedings. Where intelligence identifies information relevant to a criminal case, such information must subsequently be verified and, where necessary, obtained or reproduced through procedures consistent with applicable criminal procedural and evidentiary requirements. This distinction is essential to ensure that intelligence can support early detection without bypassing due process of law. Therefore, reconstruction requires regulatory harmonization, clear functional boundaries, legally regulated data interoperability, standards for AI-assisted analysis, human review of automated outputs, judicial control over intrusive measures, and an effective accountability mechanism.

Police Intelligence Failures in Respect of Legal Certainty, Accountability, and Human Rights Protection

The failure of police intelligence to detect and anticipate transnational crime not only reflects the weak technical capacity of law enforcement institutions but also indicates serious problems with legal certainty, accountability, and human rights protection within the national legal system. In a state based on the rule of law, as affirmed in Article 1 paragraph (3) of the 1945 Constitution of the Republic of Indonesia, every action by law enforcement officers must be based on the principles of legality, due process of law, and respect for the constitutional rights of citizens. However, police intelligence practices in Indonesia often face issues of unclear norms, weak oversight, and irregular decision-making mechanisms, creating legal uncertainty in the law enforcement process against transnational crime. The increasing number of international narcotics crimes, transnational cybercrime, human trafficking, and terrorist financing demonstrates that the intelligence system is not yet capable of functioning optimally as an early warning system in detecting threats to national security. In numerous empirical cases, law enforcement officials are often late in identifying patterns of international criminal networks, resulting in action only after the crimes have spread widely and caused serious social impacts. This situation demonstrates that intelligence failures are not solely operational in nature, but are also closely related to weaknesses in the legal system, which has failed to establish effective, accountable, and human rights-based intelligence mechanisms.

From a legal certainty perspective, the primary weakness of police intelligence lies in the lack of clarity regarding the limits of authority, the use of intelligence information, and decision-making mechanisms within the law enforcement system. Article 14 paragraph (1), letter g of Law Number 2 of 2002 concerning the Indonesian National Police authorizes the National Police to conduct inquiries and investigations into all criminal acts, while Article 6 of Law Number 17 of 2011 concerning State Intelligence regulates the functions of investigation, security, and mobilization within the framework of national security. However, neither regulation provides clear provisions regarding the legality of using intelligence findings as a basis for law enforcement decisions or the boundaries between intelligence and investigative functions. As a result, overlapping authorities and unclear procedures often occur in practice, weakening the effectiveness of early detection of transnational crime. Empirically, the escape of international narcotics networks through sea routes and borders, the rise of cross-border cyberattacks on national digital systems, and the rise in cryptocurrency-based money laundering activities demonstrate that intelligence systems still experience analytical delays and poor information integration between agencies. This situation creates legal uncertainty because law enforcement decisions are often not based on measurable and accountable intelligence standards, but rather are reactive after a crime has occurred.

The next problem relates to weak accountability within the police intelligence system, which often results in a lack of transparency in decision-making processes and difficulty in legal oversight. In a democratic state, the use of intelligence authority must be subject to the principle of checks and balances to prevent abuse of power. However, Indonesian regulations still lack comprehensive provisions on intelligence audit mechanisms, decision-making evaluation parameters, or forms of legal accountability for intelligence failures.

Article 31 of Law Number 17 of 2011 grants state intelligence the authority to wiretap based on statutory provisions, but this norm lacks detailed regulations regarding judicial authorization, oversight mechanisms, or limits on the use of intercepted data. As a result, intelligence processes often occur behind closed doors without adequate control mechanisms. Empirically, numerous cases of data leaks, weak oversight of cross-border digital activity, and delays in identifying terrorist financing demonstrate the failure of the intelligence oversight system to anticipate threats preventively. In some cases, the use of intelligence authority without accountability parameters has the potential to lead to discriminatory actions, excessive profiling, and the misuse of individuals' personal data. This demonstrates that weak intelligence accountability not only impacts the effectiveness of national security but also has the potential to threaten the principles of the rule of law and constitutional democracy.

From a human rights perspective, police intelligence failures also raise serious issues related to privacy protection, civil liberties, and ensuring public security. Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia affirms that everyone has the right to protection of themselves, their families, their honor, their dignity, and their security, while Article 28D paragraph (1) guarantees the right to recognition, protection, and fair legal certainty. Likewise, Law Number 39 of 1999 concerning Human Rights also emphasizes that the state is obliged to respect and protect citizens' rights to privacy and freedom from arbitrary action. However, police intelligence practices that are not supported by effective oversight mechanisms have the potential to lead to uncontrolled surveillance, wiretapping without clear parameters, and excessive collection of personal data. Furthermore, intelligence failures in detecting transnational crime threats also have a direct impact on human rights violations, resulting in increased human trafficking, sexual exploitation, drug trafficking, and cyber-attacks on citizens' personal data. Thus, intelligence weaknesses create two risks simultaneously: the state's failure to protect the public from the threat of transnational crime and the potential for human rights violations resulting from the uncontrolled use of intelligence powers.

The failure of police intelligence also demonstrates the gap between "*das sollen*" (the principle of truth) and "*das sein*" (the principle of truth) in the national law enforcement system. Normatively, police intelligence should be a strategic instrument that operates quickly, accurately, in an integrated manner, and is based on modern technology to support intelligence-led and predictive policing in addressing the development of transnational crime. However, empirical reality shows that the intelligence system remains sectoral and bureaucratic, and is unable to integrate data across law enforcement agencies. Database fragmentation, low big data analysis capacity, weak international coordination, and minimal information system interoperability often result in slow decision-making and a lack of comprehensive risk analysis. This situation contrasts with practices in several developed countries, such as the Federal Bureau of Investigation, Europol, and the Australian Federal Police, which have developed integrated criminal intelligence systems based on artificial intelligence and real-time intelligence sharing. This gap demonstrates that the police intelligence system in Indonesia still faces legal and implementation gaps, hampering the

effectiveness of early detection and strategic decision-making regarding modern transnational crime threats.

Based on these various issues, it is understandable that the failure of police intelligence in terms of legal certainty, accountability, and human rights protection is fundamentally a consequence of the weak construction of the national intelligence legal system, which has not been able to adapt to the developments of modern transnational crime. Therefore, reconstruction of the police intelligence legal system is necessary through regulatory harmonization, strengthening the legality of intelligence-based decision-making, establishing an independent oversight mechanism, and developing an integrated intelligence system based on modern analytical technology. This reform must be directed at creating an intelligence system that is not only effective in detecting and preventing transnational crime but also guarantees the principles of due process of law, legal certainty, accountability, and respect for human rights, as mandated by the 1945 Constitution of the Republic of Indonesia. Therefore, reform of the police intelligence system is an urgent need to build a modern, democratic, and adaptive law enforcement system to the increasingly complex dynamics of global threats.

Reconstruction of the Police Intelligence Legal System Based on Predictive Policing and an Integrated Criminal Intelligence System in Combating Transnational Crime

The reconstruction of the police intelligence legal system in combating transnational crime should be directed toward establishing a legally bounded predictive and integrated criminal intelligence framework rather than merely introducing new technologies into existing practices. Conventional intelligence-led policing remains relevant as a framework in which intelligence supports strategic and operational decision-making. Predictive policing, however, constitutes a more specific analytical mechanism that uses integrated data, pattern recognition, and risk assessment to identify potential threats before they materialize. Accordingly, predictive policing should operate within, rather than replace, intelligence-led policing. Its legal reconstruction must therefore regulate not only the use of technology but also the limits of automated analysis, the role of human decision-makers, the protection of personal data, and the mechanisms through which intelligence outputs may be translated into lawful law-enforcement action.

Normatively, these reforms should be based on Article 30 paragraph (4) of the 1945 Constitution of the Republic of Indonesia and Article 13 of Law Number 2 of 2002 concerning the Indonesian National Police, while amendments to Law Number 2 of 2002 and Law Number 17 of 2011 should provide an explicit legal basis for predictive intelligence and AI-assisted analysis. The proposed legal framework should define predictive policing as the use of lawfully obtained and relevant information to identify patterns, assess risks, and support preventive and strategic law-enforcement decisions. The law should expressly provide that predictive outputs constitute decision-support tools and may not independently authorize arrest, prosecution, interception, search, or other coercive measures. Any such measure must remain based on legally established authority, objectively verifiable information, proportionality, and human decision-making. The proposed amendments should also require that AI systems used for intelligence purposes

be subject to documented governance procedures, including identification of the responsible institution, specification of the intended purpose, limitations on the categories of data processed, security requirements, retention periods, periodic accuracy assessments, and mechanisms for independent auditing.

In addition to data integration, the reconstruction must establish specific legal standards governing the use of artificial intelligence, big data analytics, facial recognition, and automated risk assessment. Data processing for predictive intelligence should be limited by the principles of legality, specified purpose, necessity, proportionality, data minimization, accuracy, security, access control, and retention limitation. The collection of personal data should be limited to information that is demonstrably relevant to a legitimate intelligence objective, and data should be deleted or anonymized when its retention is no longer necessary for the legally defined purpose. The use of facial recognition and other high-risk technologies should be subject to stricter authorization and documentation requirements because of their potential impact on privacy and freedom from discriminatory treatment. Automated risk assessment must also remain subject to meaningful human review. Before any high-risk AI system is deployed, the responsible institution should conduct a legal and human-rights impact assessment addressing potential bias, discrimination, error rates, false positives, and risks of unlawful profiling. The system should subsequently undergo periodic independent audits, and every significant AI-assisted decision should be supported by an auditable record capable of showing the data basis, analytical output, human validation, and subsequent action.

Furthermore, the reconstruction of the police intelligence legal system must be strengthened through enhanced international cooperation in combating transnational crime. The nature of transnational crime requires rapid and legally regulated information exchange across jurisdictions, but international cooperation should also comply with the principles governing data protection, purpose limitation, institutional accountability, and the lawful use of intelligence information. Therefore, the expansion of mutual legal assistance, extradition, and intelligence-sharing arrangements should be accompanied by clear rules concerning the categories of information that may be exchanged, the receiving authority, the permitted purpose of use, security obligations, and restrictions against the unauthorized onward transfer of information. Indonesia should also strengthen cooperation with ASEAN countries and relevant international organizations in addressing cybercrime, human trafficking, international narcotics trafficking, terrorist financing, and other forms of transnational organized crime. This step aligns with the 2000 United Nations Convention against Transnational Organized Crime, ratified through Law Number 5 of 2009, which emphasizes the importance of international cooperation in eradicating transnational organized crime. The development of international data interoperability should therefore be accompanied by legal safeguards ensuring that accelerated information exchange does not weaken domestic constitutional protections.

Reconstructing the police intelligence legal system based on predictive policing and an integrated criminal intelligence system therefore requires a more specific statutory transformation than the simple adoption of artificial intelligence or big data technology.

Amendments to Law Number 2 of 2002 and Law Number 17 of 2011 should expressly regulate: the legal definition and permissible scope of predictive policing; the distinction between intelligence information and criminal evidence; standards governing data collection, processing, access, retention, and interoperability; the prohibition of fully automated coercive decisions; mandatory human review of AI-assisted outputs; pre-deployment assessments and periodic independent algorithmic audits; judicial authorization for intrusive surveillance; time limitations and renewal procedures; emergency exceptions subject to subsequent judicial review; and an independent oversight mechanism with effective audit and corrective powers. Through these provisions, predictive policing can function as a legally regulated analytical instrument within intelligence-led policing rather than as an autonomous technological system. The reconstruction is therefore directed toward creating an intelligence framework that is preventative and predictive while remaining transparent in its legal basis, traceable in its decision-making, accountable in its exercise of authority, and consistent with the protection of human rights and the principles of a democratic state based on the rule of law.

Conclusion

Based on the discussion, it can be concluded that the weaknesses of the police intelligence legal system in detecting and making decisions regarding transnational crime are caused by regulatory disharmony, weak integration of intelligence data, unclear boundaries of authority, low accountability in decision-making, and suboptimal protection of human rights in police intelligence practices. The development of borderless, organized, and high-tech transnational crime has demonstrated that conventional repressive and reactive law enforcement approaches are no longer capable of addressing the complexity of modern security threats. The failure of police intelligence to detect international narcotics networks, transnational cybercrime, human trafficking, terrorist financing, and money laundering demonstrates legal and implementation gaps in the national intelligence legal system. Furthermore, weak inter-agency coordination, database fragmentation, limited risk analysis, and minimal oversight mechanisms often result in ineffective, unintegrated intelligence decision-making processes that have the potential to lead to human rights violations. Therefore, the reconstruction of the police intelligence legal system based on predictive policing and an integrated criminal intelligence system is urgently needed to realize a modern, preventative, predictive, accountable, and equitable law enforcement system in response to the development of modern transnational crime.

Based on these conclusions, this study recommends the need to update and harmonize regulations governing police intelligence through a revision of Law Number 2 of 2002 concerning the Indonesian National Police and Law Number 17 of 2011 concerning State Intelligence to accommodate the development of predictive policing, the use of artificial intelligence, big data analytics, and intelligence-based decision-making mechanisms that have clear legal certainty and accountability. Furthermore, the establishment of an integrated criminal intelligence system is necessary through the development of a national intelligence data integration center that connects the Indonesian National Police, the National Narcotics Agency, the Financial Transaction Reports and Analysis Center

(PPATK), Immigration, Customs and Excise, and other related institutions in real time to improve the effectiveness of early detection of transnational crime. The state must also establish an independent oversight mechanism and judicial control over the use of intelligence authority to prevent abuse of power and ensure the protection of human rights in accordance with the principles of a democratic state based on the rule of law. Furthermore, increasing the capacity of human resources in police intelligence, strengthening international cooperation, and developing a cyber-intelligence system and a transnational crime predictive task force are strategic steps that must be taken so that police intelligence can transform into a modern security system that is adaptive, professional, and responsive to the dynamics of global threats in the future.

References

Arif, M. (2021). Tugas Dan Fungsi Kepolisian Dalam Perannya Sebagai Penegak Hukum Menurut Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian. *Al-Adl : Jurnal Hukum*, *13*(1), 91. https://doi.org/10.31602/al-adl.v13i1.4165

Debora, A., Kambuno, A., & Pabeangi, J. D. (2025). TINJAUAN HUKUM TERHADAP RUU POLRI : EFEKTIVITAS PENEGAKAN HUKUM DAN RISIKO PENYALAHGUNAAN WEWENANG Rancangan Undang-Undang tentang Kepolisian Negara Republik Indonesia. *Jurnal Multilingual*, *5*(1), 416–425.

Harefa, H. (2018). Optimalisasi Fungsi Intelijen Kepolisian dalam Penyelidikan Tindak Pindana Narkotika yang Dilakukan Anggota Kepolisian (Studi Sat Intelkam Polres Solok). *UNES Law Review*, *1*(1), 44–52.

Husen, L. O., Salle, S., Syalman, A. A., & Muzakkir, A. K. (2020). Efektivitas Pengamanan Intelijen Kepolisian Terhadap Putusan Pengadilan Atas Objek Sengketa. *SIGn Jurnal Hukum*, *1*(2), 136–148. https://doi.org/10.37276/sjh.v1i2.62

Insani, N. S., Mulyana, R. N., & Hosnah, H. A. U. (2026). Dampak perubahan sosial terhadap pola kejahatan: Perspektif kriminologi. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *4*(1), 3116–3176. https://doi.org/10.61104/alz.v4i1.3610

Ismail, M. (2023). Digital Policing ; Studi Pemanfaatan Teknologi Dalam Pelaksanaan Tugas Intelijen Kepolisian untuk Mencegah Kejahatan Siber (Cybercrime). *Jurnal Ilmu Kepolisian*, *17*(3), 15. https://doi.org/10.35879/jik.v17i3.428

Matompo, S., & Lestiawati, I. (2025). TINJAUAN YURIDIS PERAN INTELIJEN KEMANAN KEPOLISIAN DALAM MELAKUKAN DETEKSI DINI TERHADAP TERJADINYA KONFLIK SOSIAL (Studi Kasus di Wilayah Hukum Kepolisian Daerah Sulawesi Tengah) OVERVIEW OF JURIDICAL ROLE IN POLICE SECURITY INTELLIGENCE IN CONDUCTING EARLY DETECTION OF SOCIAL CONFLICT (Case study in central Sulawesi regional Police Jurisdiction) 1 I Putu Agus Sugianto, 2 Osgar. *Jurnal Kolaboratif Sains*.

Naseh, M. (2019). Karakteristik Pelaku Kejahatan Transnasional Terorganisir di Indonesia dan Eropa. *Jurnal Hubungan Internasional*, *8*(1), 48–60. https://doi.org/10.18196/hi.81144

Pohan, A. P. (2025). Optimalisasi Pendekatan Intelligence-Led Policing Untuk Menekan Tindak Kriminalitas Berulang: Studi Di Polresta Samarinda. *Menulis: Jurnal Penelitian Nusantara*, *1*(10), 345–358.

https://padangjurnal.web.id/index.php/menulis/article/view/695

Pramawi Nicolas Huliselan. (2023). Peran Intelijen Kepolisian Sebagai Tindakan Preventif Dalam Menanggulangi Tindak Pidana Cyber Crime. *Paulus Law Journal*, *5*(1), 64–87. https://doi.org/10.51342/plj.v5i1.733

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. *Healthcare (Switzerland)*, *8*(2). https://doi.org/10.3390/healthcare8020133

Sirait, S., & Abdillah, J. (2025). Peran Intelijen Keamanan Dalam Pencegahan Dan Penanggulangan Tindak Pidana Terorisme. *Jurnal Usm Law Review*, *8*(2), 673–686. https://doi.org/10.26623/julr.v8i2.11952

Tabiu, R., Heryanti, Intan, N., & Safiuddin, S. (2023). Globalisasi dan Kejahatan Transnasional Terorganisasi. *Halu Oleo Law Review*, *7*(1), 99–110. https://doi.org/10.33561/holrev.v7i1.11

Ubaidillah, L., Rahma, A. B., & Andriansyah, I. A. N. (2025). Diferensiasi Fungsional Kejaksaan dan Kepolisian dalam Integrated Criminal Justice System (ICJS). *Fairness and Justice: Jurnal Ilmiah Ilmu Hukum*, *23*(1), 1–8.

Wirandy, M. A., & Syaufi, A. (2025). Optimalisasi Fungsi Intelijen Kepolisian Dalam Penanganan Kejahata Terorganisir Transnasional Optimizing the Function of Police Intelligence in Combating Transnational Organized Crime. *Jurnal Kolaboratif Sains*, *8*(6), 3584–3596. https://www.jurnal.unismuhpalu.ac.id/index.php/JKS/article/download/7871/5555/

Wulandari, S., & Tofan, A. A. (2026). Efektifitas Intelijen Kepolisian Dalam Mengantisipasi Gangguan Keamanan Di Masyarakat. *Spektrum Hukum*, *22*(2), 136. https://doi.org/10.56444/sh.v22i2.6990