



Research Article

Predictive Policing Models to Detect and Reveal Crime in the Digital Era

Deki Marizaldi^{1*}, M. Herdi Pratama², Lindrianasari³, Tagor Hutapea⁴

¹Indonesian National Police, Indonesia; email: dekimarco86@gmail.com

²Indonesian National Police, Indonesia; email: herdi.den45@gmail.com

³Indonesian National Police, Indonesia; email: lindrianasari17@gmail.com

⁴Indonesian National Police, Indonesia; email: tagor.hutapea@gmail.com

*Corresponding Author: dekimarco86@gmail.com

Abstract: This study aims to provide a comprehensive analysis of Predictive Policing and its implications for law enforcement transformation in Indonesia, based on an extensive review of its global applications, benefits, and challenges. The study uses qualitative literature and international case study review methods to assess the impact and complexity of implementing digital technologies such as artificial intelligence (AI), machine learning, and big data analytics within a Predictive Policing framework. The results of this review highlight that while Predictive Policing offers significant potential for proactive crime prevention and increased operational efficiency, its implementation is consistently fraught with critical legal, ethical, and technical challenges, including regulatory gaps, risks of algorithmic bias, and data privacy concerns, which are particularly relevant to Indonesia. The findings underscore that public trust and police legitimacy in the context of adopting such technologies are strongly influenced by transparency, strong accountability mechanisms, and community involvement in shaping their use. This study contributes to the growing discourse on digital policing in developing countries and culminates in practical policy recommendations designed to guide the Indonesian police towards the development and implementation of Predictive Policing models that are effective, efficient, and fundamentally respectful of legal and human rights principles.

Keywords: AI in Law Enforcement; Big Data Analytics; Police Legitimacy; Predictive Policing; Public Trust.

1. Introduction

The development of digital technology has brought significant changes in various aspects, including the police system and law enforcement practices. In facing the increasingly complex development of crime in the digital era, especially with the increasing number of cyber attacks in Indonesia, innovations such as Predictive Policing (PP) have emerged as a crucial approach. PP utilizes artificial intelligence (AI), machine learning, and big data analysis from various sources to predict and anticipate potential criminal acts proactively, offering an alternative to traditional methods that tend to be reactive. Although PP promises increased efficiency in detecting and preventing crime, its implementation also poses new and complex challenges, especially related to privacy issues, the ethics of managing sensitive data, potential algorithmic bias, and its impact on public trust and the relationship between police institutions and the community.

Artificial intelligence (AI) and machine learning to analyze crime patterns based on historical data. The data used includes previous crime reports, CCTV footage, social media, and suspicious financial transactions. By using predictive analysis, the system can provide early warnings to law enforcement officers regarding the potential for criminal acts in certain locations or involving certain individuals (Windani, 2023). Therefore, Predictive Policing not

Received: 11 December 2025

Revised: 16 January 2026

Accepted: 01 February 2026

Published: 02 February 2026

Curr. Ver.: 02 February 2026



Copyright: © 2025 by the authors.

Submitted for possible open

access publication under the

terms and conditions of the

Creative Commons Attribution

(CC BY SA) license

([https://creativecommons.org/li](https://creativecommons.org/licenses/by-sa/4.0/)

[censes/by-sa/4.0/](https://creativecommons.org/licenses/by-sa/4.0/))

only focuses on disclosing crimes that have already occurred, but also aims to prevent crimes from occurring, which ultimately increases efficiency in law enforcement.

In the digital era, various types of crimes continue to develop and change, both in patterns and modus operandi, especially with the emergence of technology-based crimes. Cybercrime, digital fraud, illicit trade on the dark web, and digital money laundering are now new challenges for law enforcement. Based on data (Kominfo, 2025), it was recorded that Indonesia experienced 370.02 million cyber attacks in 2022. This figure increased by 38.72% compared to the previous year which recorded 266.74 million attacks. The government administration sector is the main target of cyber attacks in Indonesia, with a total of 284.09 million attacks. These cyber attacks include: 1) Phishing: online fraud that tries to obtain personal information such as passwords and credit card numbers. 2) Ransomware attacks: attacks that encrypt data and require victims to pay a ransom to regain access. 3) Malware: malicious software that can damage systems and steal data. 4) Distributed Denial of Service (DDoS) attack: an attack on a server or network by flooding it with traffic, making it unavailable to legitimate users. 5) Man in the Middle (MITM) attack: intercepting communications between two legitimate parties and stealing information as it is transmitted. 6) Zero-Day attack: an attack that exploits a software vulnerability that has not been discovered or reported to the developer. These attacks can be very damaging because there are no security updates available. 7) Identity attack: stealing someone's personal information, such as credit card numbers or identification data, and using it for illegal purposes. 8) Web application attack: exploiting a web application to steal user data or gain access to a server.

In the 2024 year-end release report delivered directly by the National Police Chief General Pol. Listyo Sigit Prabowo, quoting from (Kompas, 2025), the National Police Chief General Pol. Listyo Sigit Prabowo reported that throughout 2024, the National Police uncovered 3,331 cases of cybercrime. The cybercrimes that were uncovered were of various types, ranging from fraud, defamation, pornography, hoaxes, hate speech, illegal access, data theft, hacking, illegal wiretapping, to data theft.

This phenomenon requires law enforcement agencies in Indonesia, especially the Police, to develop new strategies in dealing with virtual crimes. For example, the police in several countries have formed special units that focus on handling cybercrimes. This unit is not only equipped with sophisticated technology, but must also have personnel who are trained in information technology and cybersecurity.

This increasingly sophisticated crime mode demands a more adaptive and technology-based approach in identifying and exposing perpetrators of crimes. Predictive Policing is present as a solution that is expected to be able to answer these challenges by optimally utilizing data in order to prevent and eradicate crime.

Although Predictive Policing offers many advantages in law enforcement, its implementation also brings major challenges, especially in terms of law and ethics. One of the most striking problems is the potential for violations of people's privacy rights. The use of surveillance technologies such as facial recognition, social media analysis, and real-time location tracking can raise serious concerns about human rights and personal data protection (Dirgala, Basir, and Nita, 2023). In addition, Predictive Policing also risks creating unfair and biased profiling in algorithms, which can ultimately lead to discrimination against certain groups or individuals.

From a legal perspective, Predictive Policing poses challenges related to its compliance with the principles of due process of law and the presumption of innocence. In the criminal law system, a person can only be prosecuted based on valid and strong evidence. However, because Predictive Policing is predictive, law enforcement officers can take action based on the possibility of a crime that has not necessarily occurred. This risks contradicting the principle of *nullum crimen sine lege* which states that a person can only be punished if they have committed a crime regulated by law. Therefore, the legal aspects of Predictive Policing need to be studied in depth so that they do not conflict with the principles of justice in the criminal justice system. In addition to the legal and ethical aspects, another challenge in implementing Predictive Policing is the technical aspect, especially related to data quality and the potential for bias in artificial intelligence algorithms. Predictive Policing is highly dependent on the quality of the data used in the analysis. If the data entered contains bias or is incomplete, the results of the analysis can be inaccurate and risk causing errors in decision

making. For example, if crime data comes more from a particular area, Predictive Policing tends to focus law enforcement on that area, even though it may not reflect the true picture of crime (Hutama et al., 2023).

In addition, Predictive Policing also faces threats related to data security and potential cyber attacks. Systems that rely on big data and AI analysis are vulnerable to manipulation and hacker attacks that can damage data integrity or even falsify analysis results. If the Predictive Policing system is infiltrated by irresponsible parties, inaccurate analysis results can lead to wrong decisions by law enforcement officers. Therefore, it is very important to have a strict data security mechanism and transparent supervision of the use of Predictive Policing so that this technology can be implemented effectively and responsibly.

In terms of policy, the implementation of Predictive Policing also requires a clear and comprehensive regulatory framework. In Indonesia, the use of AI-based technology in the criminal justice system does not yet have a strong legal basis. The Electronic Information and Transactions Law (UU ITE) and regulations related to personal data protection are legal references that can be used to regulate the implementation of Predictive Policing. However, specific regulations are needed that explicitly regulate the limitations of the use of Predictive Policing, the standards for algorithm accuracy, and accountability mechanisms for officers who use it.

Despite facing various challenges, Predictive Policing still has the potential to be an innovative solution to improve the effectiveness of law enforcement in the digital era. In several developed countries, such as the United States, England, and Singapore, Predictive Policing has been implemented with significant results in reducing crime rates. However, the implementation of this technology must be accompanied by policies that guarantee transparency, accountability, and respect for human rights.

This study focuses on an in-depth analysis of the concept, mechanisms, and various multidimensional challenges in the implementation of Predictive Policing, with a special emphasis on the Indonesian context. Given the ever-evolving and increasingly sophisticated modes of crime that demand adaptive technological solutions, PP offers this potential. However, this study identifies that its implementation faces fundamental legal challenges, such as the absence of a specific PP regulatory framework and the problem of its compliance with the principles of due process and the principles of criminal justice in Indonesia. Furthermore, ethical aspects related to potential violations of privacy rights and the risk of discrimination due to systemic bias in data or algorithms, as well as technical challenges related to the validity of data quality and cybersecurity threats, are central issues that require comprehensive studies to ensure that every application of this technology can be accounted for and does not harm the human rights of citizens.

This study aims to develop a comprehensive and responsible conceptual model for the implementation of predictive policing in the Indonesian context, by deeply analyzing the concept, working mechanisms, and the multidimensional challenges that accompany it. Although various studies have examined aspects of predictive policing, this study offers something new through its holistic analysis coverage covering legal, ethical, and technical dimensions in an integrated manner and its focus on formulating a framework (Input-Process-Output correlated with SWOT) and policy recommendations that are specifically tailored to the legal system, socio-cultural conditions, and technological capabilities in Indonesia. Thus, this study builds on the foundation of existing literature, but provides a unique contribution to the adaptation and strategic implementation of predictive policing at the national level.

The case study conducted by (Dirgala et al., 2023) provides an important contribution by presenting empirical evidence on the application of predictive policing to prevent child brawls in the jurisdiction of the South Jakarta Metro Police. Although this study provides valuable insights at the micro level and for certain types of crimes in certain jurisdictions in Indonesia, this study takes a more macro and comprehensive perspective. Its novelty lies in the effort to not only analyze a single case of implementation, but also to develop a national framework model that can be applied more broadly to various types of crimes in various regions in Indonesia. The focus is on the design of systems and regulations at the policy level, which goes beyond the operational analysis of a single case study.

Furthermore, this study also distinguishes itself from international studies such as those conducted by (Alikhademi et al., 2022) and (Benbouzid, 2019). (Alikhademi et al., 2022) presents an in-depth literature review on predictive policing from a justice perspective. Although aspects of justice and algorithmic bias are also important concerns in this study, the scope of the analysis is expanded to cover a broader spectrum of ethical challenges, as well as legal and technical challenges relevant to the Indonesian context. Meanwhile, (Benbouzid, 2019) explores predictive policing practices in the United States with a focus on prediction and management aspects. On the other hand, this study emphasizes the development of a model that is tailored to the legal, social, infrastructure, and specific needs of Indonesia, rather than simply adopting or criticizing models centered in other countries.

Thus, the main novelty of this research lies in three fundamental aspects. First, the development of a "Thinking Framework" model that integrates the Input-Process-Output approach with a SWOT analysis to map and evaluate the predictive policing system holistically. Second, an in-depth analysis of the multidimensional challenges (legal, ethical, technical) contextualized for Indonesia, including an analysis of existing national regulations and their development needs. Third, a strong research orientation on the formulation of concrete policy recommendations and applicable regulatory frameworks, with the ultimate goal of guiding the implementation of predictive policing that is not only effective and efficient, but also fair, transparent, accountable, and respects human rights in the law enforcement system in Indonesia.

This research has significant theoretical and practical benefits. Theoretically, this research is expected to enrich the scientific literature on the adoption of Predictive Policing technology and its governance aspects, especially in the context of developing countries like Indonesia that have unique challenges in implementing advanced technology. By conducting a comprehensive analysis of the concept, working mechanism, along with the accompanying legal, ethical, and technical challenges, this research aims to provide a deeper understanding of the dynamics and implications of PP implementation. In practice, the findings and policy recommendations resulting from this study are designed to be a constructive reference for the Indonesian National Police (Polri) and other relevant stakeholders in formulating a regulatory framework and guidelines for the implementation of PP that are more adaptive, effective, efficient, and always in line with legal principles and respect for human rights.

The main basis of this research is based on the urgent need to bridge the enormous potential offered by Predictive Policing technology in improving law enforcement performance in the digital era with the need to manage its various risks and challenges carefully and responsibly. Amidst the changing landscape of security and law enforcement triggered by technological disruption, it is important to understand how the National Police can utilize this innovation effectively without sacrificing fundamental values such as justice, transparency, accountability, and excellent public service, all of which are the foundation of the legitimacy of the police institution. Therefore, this research seeks to provide an important contribution to the development of a model or framework for the implementation of Predictive Policing in Indonesia that is not only technologically and operationally superior, but also legally and ethically sound, and fully accountable to the wider community.

2. Materials and Method

This study uses a combination of qualitative and quantitative approaches. The qualitative approach is used to analyze case studies of predictive policing implementation in various countries, focusing on the legal and ethical challenges that arise. Meanwhile, the quantitative approach is used to analyze historical data related to criminal acts, including technology-based crimes. This study also includes regression analysis to evaluate the level of accuracy of the algorithm used in predicting criminal acts. 1) Literature Study: Collecting and analyzing various relevant literature on predictive policing, such as journal articles, books, and previous research reports. This step aims to build a strong theoretical foundation in understanding the concept and how predictive policing works. 2) Qualitative Analysis: Conducting qualitative analysis of data obtained from case studies of predictive policing implementation in various countries, highlighting the challenges faced and the results obtained. This process can involve interviews with legal practitioners, law enforcement officers, and technology experts to gain deeper insights. 3) Data Analysis: Using data analysis techniques to assess historical crime

patterns and perpetrator behavior, and identify potential biases in the algorithms applied in predictive policing. 4) Policy Recommendation Development: Based on the results of the qualitative analysis and case studies, this study will formulate policy recommendations that can assist in the development of a clear and comprehensive regulatory framework regarding the use of predictive policing in Indonesia. Through this approach, this study is expected to provide a significant contribution to the understanding and application of predictive policing in law enforcement in the digital era.

3. Results and Discussion

To analyze the complexity of predictive policing implementation in Indonesia and formulate a comprehensive model, this study adopts a framework that integrates the Input-Process-Output (IPO) model with SWOT analysis. This approach was chosen because of its ability to structurally dissect the system through IPO, while evaluating internal and external factors that influence it through SWOT, especially at the core process stage. This framework aims to provide a strong foundation in understanding how predictive policing can be planned, implemented, and managed effectively and responsibly in Indonesia.

The IPO model in concept (Von Bertalanffy, 1968) is applied to systematically map the workflow of the predictive policing system. The inputs in this model include all resources and basic elements that are crucial to starting and running the system, such as various types of data (criminal history, CCTV, social media, financial transactions), advanced technology (Artificial Intelligence/AI, Machine Learning/ML, Big Data Analysis), competent Human Resources (HR) (trained officers, data analysts, IT experts), adequate budget, institutional commitment from law enforcement agencies, and supporting technology and network infrastructure. Furthermore, the Process describes the transformation of these inputs through a series of core stages that include “System Planning & Development” (requirements analysis, model design, algorithm development, SOP preparation), “Implementation & Operationalization” (continuous data collection, analysis and prediction, intelligence generation, and deployment for field actions such as targeted patrols and proactive interventions), and “System Management & Oversight” (performance monitoring, ethical and legal audits, system security, human resource training, and ongoing evaluation). Finally, Outputs are the expected outcomes and impacts of the system, including accurate crime predictions, timely criminal intelligence, increased police operational efficiency and effectiveness, potential crime reductions, and increased public trust and safety. The IPO structure is consistent with the basic principles of General Systems Theory and commonly used systems analysis methodologies for understanding complex information technology systems (Clark, 2014).

Result

Framework of Thinking

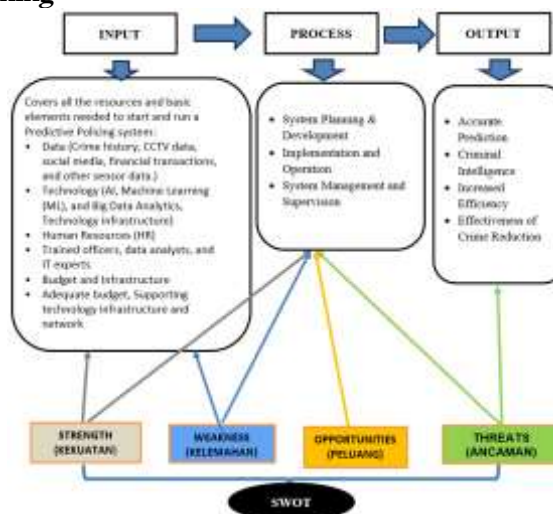


Figure 1. Predictive Policing Model for Indonesia.

To complement the structural analysis of the IPO, a SWOT analysis cited through the concept in Strategic Management (White, 2017) is integrated to evaluate the contextual factors that influence, especially in the Process block. SWOT identifies Strengths and Weaknesses as

internal factors inherent in the system or the institution's ability to carry out the predictive policing process. Opportunities and Threats are identified as external factors originating from the operational, technological, social, and policy environments. The use of SWOT analysis in this context is based on strategic management literature that emphasizes the importance of understanding the internal and external environment for effective strategy formulation and system management.

Within the framework of the developed predictive policing model, Strength is understood as a positive internal factor that is inherent and becomes the foundation for the entire system. This strength is manifested in the superior quality of various Input components, such as the availability of rich and accurate historical data, advanced technologies such as qualified Artificial Intelligence (AI) and Machine Learning (ML), competent and trained Human Resources (HR), and adequate supporting infrastructure. Furthermore, Strengths are also reflected in the effectiveness and efficiency of the Process itself, for example in a mature "System Planning & Development", proper "Implementation & Operationalization", or solid "System Management & Monitoring". Therefore, Strengths are not depicted as external elements that "influence" Inputs or Processes, but rather as intrinsic attributes that enable quality Inputs and become an integral part of an effective Process, ultimately contributing to the achievement of the desired Outputs. (Skyttner, 2005)

In contrast, Weaknesses, which are also internal factors, are visually and conceptually depicted as having a direct impact on Inputs and ultimately on the Process. The arrows from "Weaknesses" pointing to "Process" in the model indicate that various internal deficiencies or limitations can significantly hinder, complicate, or reduce the quality of the various stages in the predictive monitoring Process. These weaknesses can originate from less than optimal Inputs, such as poor quality, incomplete, or systemic biased data, limitations in the technology used, lack of human resources with specialized expertise, or inadequate infrastructure. Weaknesses in these Inputs will negatively impact the Data Analysis Process, which can result in inaccurate predictions and erroneous law enforcement decisions. (Saloner, Shepard, and Podolny, 2005)

Furthermore, Weaknesses can also be inherent in the Process itself, for example in rushed "System Planning & Development", non-standard "Implementation & Operationalization", or weak "System Management & Oversight". For example, complex and difficult-to-understand algorithms (weaknesses in the transparency aspect of the Process) can make accountability difficult. Lack of comprehensive training for officers (weaknesses in HR that impact the Process) can also lead to operational errors and bias in decision-making. Therefore, identification and mitigation of Weaknesses are essential at every stage of the Input and Process to ensure that the predictive policing system can run effectively, fairly, and achieve the desired Output without causing unforeseen negative consequences.

The critical interactions between SWOT and Process in this framework are as follows: Internal Strengths, such as the availability of advanced AI technology or skilled human resources, are the basic capital that enables and strengthens the implementation of each stage in the Process. Conversely, Internal Weaknesses, such as poor data quality, infrastructure limitations, or potential bias in algorithms, can directly hinder or complicate the effectiveness and fairness of the implementation and operationalization Process. The arrow from "Weaknesses" to "Process" in the model emphasizes these direct negative impacts. External Opportunities, such as the development of newer AI technologies, the availability of alternative data sources, or national policy support for the digitization of law enforcement, can be leveraged to improve and optimize the Process, as indicated by the arrow from "Opportunities" to "Process". Finally, external Threats, such as unclear regulations regarding privacy and the use of AI in Indonesia, the risk of cyberattacks on the system, or public resistance due to ethical concerns, can threaten the sustainability and legitimacy of the Process, or even emerge as a consequence of the implementation of the process itself if not properly mitigated.

This IPO model, enhanced with a SWOT analysis, provides a dynamic framework for evaluating how the core processes of predictive surveillance can be optimized by maximizing strengths and opportunities, and how strategies can be formulated to address weaknesses and threats. The justification for this integration is rooted in the need to understand not only "what" and "how" the system works (IPO), but also "why" the system might succeed or fail

in a given context, and “how” it can be strategically improved (SWOT). The literature in strategic technology management, public policy evaluation, and information systems governance often recommends this kind of integrated approach for comprehensive and actionable analysis.

In the context of this study, the “Implementation Support Framework in Indonesia” (which includes aspects of regulation, oversight, human rights protection, infrastructure development, human resource capacity building, public engagement, and ongoing evaluation) serves as a strategic derivative that emerges from understanding the interaction of IPO and SWOT. This Supporting Framework is designed to strengthen Strengths, address Weaknesses, utilize Opportunities, and mitigate Threats in the implementation of predictive policing processes in Indonesia. Thus, the proposed framework is expected to provide a strong and systematic basis for analysis, supported by references to relevant theoretical concepts and empirical findings from various case studies of predictive policing implementation globally and its specific challenges in Indonesia, as explained in the literature review of this study.

Discussion

The Concept and Working Mechanism of Predictive Policing in Detecting and Revealing Crime in the Digital Era

The development of digital technology has driven a transformation in law enforcement, allowing officers to utilize data-based technology for efficiency in preventing and revealing crimes. Predictive Policing (PP) has emerged as a technology-based solution that uses artificial intelligence (AI) (Kurnianto, 2021), big data analysis, and machine learning to detect and predict potential crimes based on historical data before they occur. This proactive approach is different from conventional reactive methods, which aim to anticipate crimes and increase the efficiency of law enforcement.

Predictive Policing works by analyzing various data such as crime reports, CCTV footage, suspicious financial transactions, social media activity, IoT sensor data, and online activity to identify recurring crime patterns and provide early warnings. This technology is present as a response to the complexity of crime in the digital era whose modes are increasingly sophisticated. There are two main approaches in PP (New Atlas, 2019): location-based, which identifies crime-prone areas such as Los Angeles and Chicago (Lum & Isacc, 2016) (Ferguson, 2016), and people-based, which identifies individuals at risk such as the National Data Analytics (NDAS) system in the UK (BestPractice.Ai, 2020).

Various technologies support Predictive Policing, including big data analytics to process large amounts of data, AI and machine learning to detect complex patterns such as in cases of digital fraud or suspicious transactions analyzed by Interpol and Europol (Europol, 2024). Geospatial analysis is used to map crime-prone areas such as in Santa Cruz California (Friend, 2012), while advanced surveillance systems such as AI-based facial recognition technology are used in China (Wikipedia, 2025), and Singapore (through HTX and PolCam) to identify and monitor suspicious behavior in public spaces and provide early warning to law enforcement (Deloitte, 2023). In Japan, systems such as VaakEye and Crime Nabi use AI to analyze CCTV footage and historical data to detect suspicious behavior and recommend patrol routes (JapanGov, 2020; u-tokyo.ac.jp, 2020). The PP process involves data collection, algorithmic analysis to find patterns or anomalies, risk mapping, and even digital footprint analysis to uncover complex crimes such as identity theft. Despite its great potential to improve law enforcement effectiveness, the application of predictive policing faces significant challenges. Key issues include the quality of the data used, the validity of the prediction algorithm, the potential for bias in AI systems, and legal and ethical issues related to protecting individual privacy and the limits of officers’ authority to access and analyze community data (Friend, 2012). Therefore, the application of this technology must be accompanied by clear regulations and strict supervision to ensure its use is responsible, fair, and respects human rights.

Legal, Ethical, and Technical Challenges in the Implementation of Predictive Policing

Predictive policing is an innovation in the law enforcement system, but it faces a number of quite complex challenges, both in terms of law, ethics, and technical aspects. Although this approach has great potential to prevent and uncover crimes in the digital era, in its implementation it still faces various obstacles that need to be overcome so that this technology can be implemented effectively without violating the principles of law and human rights. Many countries that have adopted predictive policing must face the dilemma of balancing the benefits of this technology with the protection of individual freedoms and ensuring that the legal process is carried out fairly (Seldadyo, Sudarto, and Sonta, 2022).

Although predictive policing offers great potential as an innovation in the law enforcement system to prevent and uncover crimes in the digital era, in its implementation it faces a number of quite complex challenges in terms of law, ethics, and technical aspects. These challenges require careful handling so that this technology can be implemented effectively without violating the principles of law and human rights, thus requiring countries to balance its benefits with the protection of individual freedoms and the fairness of the legal process. The main legal obstacle is the absence of clear regulations regarding the use of predictive policing in the criminal justice system, especially in Indonesia which does not yet have a specific law governing its limitations (Meijer and Wessels, 2019).

Although the ITE Law and the Personal Data Protection Law already exist in Indonesia, both has not yet accommodated in detail the use of PP as a technology-based law enforcement tool, so that the authorities do not yet have clear guidelines. The potential for violations of privacy rights due to the collection and analysis of big data from various sources, such as CCTV, social media, and banking transactions, is a serious obstacle, especially without adequate supervision, which can lead to data misuse and monitoring without a legal basis. This concern is further amplified in a country like Indonesia, where personal data protection regulations are considered not yet strict. Furthermore, the risk of discrimination and legal profiling due to algorithmic bias based on systematically biased historical data can unfairly target certain groups. From a criminal procedure law perspective, issues arise related to the principle of due process, the use of predictive data as evidence, and the potential for violations of the presumption of innocence and *nullum crimen sine lege* if legal action is based solely on predictions without valid evidence (Strikwerda, 2021). Ethically, algorithmic bias can lead to unfairness in law enforcement, reinforce social stereotypes, and increase public distrust, as demonstrated by case studies in the United States showing the targeting of minority groups. Lack of transparency and accountability are also significant issues; complex algorithms are often difficult to understand, making it difficult to determine responsibility for prediction errors or misuse of data. Therefore, independent oversight mechanisms are essential. Another ethical dilemma is the conflict between efforts to maintain public safety and protection of individual liberties, where PP has the potential to lead to police surveillance practices that violate civil rights if there is no proper regulation (Perry, 2013).

From a technical perspective, data validity and quality are important challenges, as biased, incomplete, or inaccurate data will result in incorrect predictions and affect decision-making. The system also requires continuous data updates to remain relevant (Ismail, 2023). The threat of cyberattacks that can compromise the integrity of the system and manipulate prediction results is also real, given the reliance on big data processing (BestPractice.AI., 2020). A strong cybersecurity system is a must. In Indonesia, technical challenges are compounded by limited technological infrastructure for big data processing, system integration between agencies, and human resource readiness for law enforcement officers, many of whom are untrained and still process data manually. To address this complexity, clear and comprehensive regulations are needed regarding the use of predictive policing in the criminal justice system. These regulations must set limits on use, protection of personal data, clear legal procedures, and strict monitoring and accountability mechanisms to prevent misuse. Transparency in the application of this technology is also important to ensure fairness and compliance with legal principles (Edco et al., 2025).

4. Conclusion

Predictive policing as a technology-based law enforcement innovation, utilizes artificial intelligence (AI), big data analysis, and machine learning to increase efficiency and effectiveness in detecting and preventing crime in the digital era. This proactive approach not only helps uncover crimes that have occurred, but also anticipates potential crimes in the future, unlike conventional reactive methods. Its application in various countries such as the United States (Los Angeles, Chicago, Santa Cruz) for mapping crime-prone areas, the United Kingdom (NDAS system) to predict at-risk individuals, China to track suspects with facial recognition, Japan (VaakEye, Crime Nabi) for CCTV analysis and suspicious behavior detection, Singapore for integrated surveillance, and Europe (Europol) to detect suspicious financial transactions, has shown significant impact. However, the application in these countries also faces criticism related to algorithmic bias, transparency, privacy, and excessive surveillance.

Despite offering many benefits, the application of predictive policing faces complex challenges from legal, ethical, and technical aspects. The main legal challenge, especially in Indonesia, is the lack of clear regulations regarding its use in the criminal justice system, where the ITE Law and the Personal Data Protection Law have not yet clearly accommodated it. From an ethical perspective, the potential for privacy violations, algorithmic discrimination due to biased data, and the lack of transparency and accountability are serious issues that can damage public trust. Technically, the validity and quality of data, the risk of cyber attacks, and the limitations of technological infrastructure and human resource readiness in Indonesia are important obstacles. Therefore, the success of the implementation of predictive policing in Indonesia is highly dependent on clear regulations, independent supervision, officer training, protection of human rights, and careful and planned implementation to create a more efficient, fair, and transparent law enforcement system.

In order for the implementation of predictive policing in Indonesia to be effective, fair, and legal, several strategic steps are needed. First, the government must immediately formulate clear and comprehensive regulations, regulating the use of this technology in law enforcement, personal data protection, and appropriate investigation and evidence procedures to ensure transparency and respect for human rights. Second, the importance of open and independent supervision by the authorities to ensure that technology is used properly, does not harm the community, maintains public trust, and prevents misuse. Third, the capacity of law enforcement officers must be improved through comprehensive training on technical and operational aspects and how to avoid algorithmic bias so that technology is used effectively and fairly.

Fourth, continuous monitoring and evaluation are needed to ensure positive impacts, identify and fix problems, and adapt technology to current developments so that it remains relevant and effective. Fifth, improving technological infrastructure is essential to support big data processing and system integration between law enforcement agencies so that predictive policing can be implemented optimally. Sixth, public involvement in development and implementation is essential to increase transparency, reduce concerns about misuse, and build a responsive legal system. Seventh, algorithmic bias management must be carried out carefully to prevent social injustice, ensure that the data used is not biased, and the system works fairly for all levels of society. With these steps and careful implementation, predictive policing has great potential to help create a more efficient, fair, transparent, and human rights-respecting legal system in Indonesia.

Acknowledgement

This research can be completed in a relatively short time due to the conducive atmosphere and intensive discussions conducted in the doctoral class of batch X at the Police Science College, Lemdiklat Polri. Thank you for the support of friends and lecturers who have provided suggestions for this research. This research is an initial research from the dissertation section, which is a graduation requirement for the doctoral program in police science at the Police Science College, Lemdiklat Polri.

Author Biography

Deki Marizaldi is a student currently pursuing a doctoral degree at the Police Science College under the auspices of the Indonesian National Police Education and Training Institute. Before pursuing a doctoral degree, the author also studied for a master's degree in Law at the Indonesian Muslim University and is currently a doctoral student in Police Science at the Police Science College, Indonesian National Police Education and Training Institute. In his police career, the author has a history of service for 12 years, currently serving as the First Police HR Assessor Level I at the HR Ro Polda Kep. Babel, effective as of April 29, 2025. With a diverse career history in the police, including various positions as Kasatreskrim at several Polres, as well as experience in development education and training such as Countering Violent Extremism, the author shows dedication to developing human resources in the Indonesian National Police environment.

M. Herdi Pratama is a student currently pursuing a doctoral degree at the Police Science College under the auspices of the Indonesian National Police Education and Training Institute. Before pursuing her doctoral degree, the author also pursued a master's degree at the University of Leeds in Transportation Planning through a scholarship from the Indonesian National Police Traffic Corps and at Diponegoro University in Law. In her police career, the author has a background as a Detective Investigator and several positions in the Indonesian National Police Traffic field. In addition, the author is also interested in the world of economics, especially the world of investment by attending several seminars to realize financial inclusion.

Lindrianasari is currently a professor at the Police Science College, Education and Training Institute, Indonesian National Police. Her expertise in research methodology and financial forensic audits has resulted in around 15 doctoral degrees, both as a promoter and as an examiner. She has also published many scientific papers in leading journals.

References

- Alikhademi, Kiana, Emma Drobina, Diandra Prioleau, Brianna Richardson, Duncan Purves, and Juan E. Gilbert. (2022). "A Review of Predictive Policing from the Perspective of Fairness." *Artificial Intelligence and Law* 1–17.
- Benbouzid, Bilel. (2019). "To Predict and to Manage. Predictive Policing in the United States." *Big Data & Society* 6(1):2053951719861703.
- BestPractice.AI. (2020). West Midlands Police anticipates violent crime with predictive policing using machine learning. BestPractice.AI. <https://www.bestpractice.ai/ai-case-study-best-practice/west-midlands-police-anticipates-violent-crime-with-predictive-policing-using-machine-learning>.
- Clark, Don. (2014). "Ludwig von Bertalanffy: General System Theory." *Online at: Http://Www. Nwlink. Com/~Donclark/History_isd/Bertalanffy. Html*.
- Deloitte. (2023). Surveillance and Predictive Policing Through AI. Diakses dari <https://www.deloitte.com/ng/en/Industries/government-public/perspectives/urban-future-with-a-purpose/surveillance-and-predictive-policing-through-ai.html>.
- Dirgala, Daniel, S. Basir, and Surya Nita. (2023). "Predictive Policing: The Future of Crime Prevention Case Study of Children Brawl in the Jurisdiction of the South Jakarta Metro Police." *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan* 2(2):531–50.
- Edco, Herman, Wijaya Simbolon, Surya Nita, and Zulkarnein Koto. (2025). "Optimization of Predictive Policing Technology for Prevention of Brawling Crimes at Bekasi City Metro Police Station." *Journal of Law, Politic and Humanities* 5(3):1447–57.
- Europol. (2024). "AI and Policing." <https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing>.
- Ferguson, A. G. (2016). Policing predictive policing. *Wash UL Rev*, 94.
- Friend, Z. (2012). Predictive Policing a Success in Santa Cruz, Calif. Government Technology. <https://www.govtech.com/public-safety/Predictive-Policing-a-Success-in-Santa-Cruz-Calif.html>.
- GovTech. (2012). Predictive policing a success in Santa Cruz, Calif. GovTech. <https://www.govtech.com/public-safety/predictive-policing-a-success-in-santa-cruz-calif.html>.

- Hutama, A. P., Runturambi, A. J. S., & Iskandar, A. (2023). The RW Police Program as an implementation of predictive policing in the legal jurisdiction of the Jakarta Metropolitan Police Department (Polda Metro Jaya). *International Journal of Multicultural and Multireligious Understanding*, 10(5), 250–258. <https://doi.org/10.18415/ijmmu.v10i5.4756>.
- Ismail, M. (2023). Digital Policing; Studi Pemanfaatan Teknologi Dalam Pelaksanaan Tugas Intelijen Kepolisian untuk Mencegah Kejahatan Siber (Cybercrime). *Jurnal Ilmu Kepolisian*, 17(3), 15–15. <https://doi.org/10.35879/jik.v17i3.428>.
- JapanGov. (2020). *Singular Perturbations develops AI-based crime prediction system in Japan*. Japan Government. <https://www.japangov.jp/2020>.
- Kominfo.(2025).“Jenis-Jenis Serangan Siber Di Era Digital.” diakses pada 11 Februari 2025 di <https://www.bpptik.kominfo.go.id/Publikasi/detail/jenis-jenis-serangan-siber-di-era-digital.html>.
- Kompas.(2025).“Cybercrime Cases Drop to 3,331 Throughout 2024.” <https://nasional.kompas.com/read/2024/12/31/15115151/kasus-kejahatan-siber-turun-menjadi-3331-sepanjang-2024>.
- Kurnianto, Thomas Agung. (2021). “Peran Kepolisian Dalam Menjaga Stabilitas Keamanan Selama Penerapan Kebijakan PSBB.” *Jurnal Ilmu Kepolisian* 15(1):11. . <https://doi.org/10.35879/jik.v15i1.291>.
- Lum, K., & Isaac, W. (2016). To Predict and Serve? Significance, 13(5), 14–19. <https://doi.org/10.1111/j.1740-9713.2016.00960.x>.
- Meijer, A., & Wessels, M. (2019). Predictive Policing: Review of Benefits and Drawbacks. *International Journal of Public Administration*, 42(12), 1031–1039. <https://doi.org/10.1080/01900692.2019.1575664>.
- New Atlas. (2019). AI-powered CCTV surveillance system detects theft behavior. <https://newatlas.com/vaak-vaakeye-ai-theft-detection/59263>.
- OpenGov Asia. (2023). PolCam's Role in Singapore's Safety Network. Diakses dari <https://opengovasia.com/2023/12/20/polcams-role-in-singapores-safety-network>.
- Perry, Walt L.(2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Rand Corporation.
- Saloner, Garth, Andrea Shepard, and Joel Podolny. (2005). *Strategic Management*. John Wiley & Sons.
- Seldadyo, Harry, Eko Rudi Sudarto, and Ahrie Sonta. 2022. “Predictive Policing: Current and Future Policing.” *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)* 5(1):3906–13.
- Skyttner, Lars. (2005). *General Systems Theory: Problems, Perspectives, Practice*. World scientific.
- Strikwerda, L. (2021). Predictive policing: The risks associated with risk assessment. *The Police Journal: Theory, Practice and Principles*, 94(3), 422–436. <https://doi.org/10.1177/0032258X20947749>.
- University of Tokyo. (2020). *Crime Nabi: AI-based crime prediction system*. University of Tokyo. <https://www.u-tokyo.ac.jp/en>.
- Von Bertalanffy, Ludwig. (1968). “General System Theory.” *New York* 41973(1968):40.
- White, Colin. (2017). *Strategic Management*. Bloomsbury Publishing.
- Wikipedia. (2025). Home Team Science and Technology Agency. Diakses dari https://en.wikipedia.org/wiki/Home_Team_Science_and_Technology_Agency
- Windani, Cynthia Ayu. (2023). “Strategi Dan Tantangan Predictive Policing Di Era Big Data Bagi Masyarakat Modern.” *Deviance Jurnal Kriminologi* 7(2):101–20.