

Predictive Policing for Hate Speech Prevention: A Study of the Indonesian National Police Cyber Directorate

Kaisan Barizi^{1*}, Riska Sri Handayani², Genoveva Ambar Wulan Tulistyowati³

¹⁻³Police Science Studies, Graduate School of Sustainable Development (GSSD), Universitas Indonesia, Jakarta, Indonesia

Email: ¹⁾ barizikaisan@gmail.com

Received : 04 June - 2026

Accepted : 08 July - 2026

Published online : 11 July - 2026

Abstract

The rise in the spread of hate speech on social media has prompted the Indonesian National Police to develop a predictive policing approach as a pre-emptive strategy for preventing cybercrime. This study aims to analyse the implementation of predictive policing in preventing the spread of hate speech on social media by the Cybercrime Directorate of the Criminal Investigation Agency (Bareskrim) of the Indonesian National Police, as well as to analyse the human resource competencies that support its implementation. The research employed a qualitative method using a phenomenological approach through in-depth interviews and a documentary study. The results indicate that predictive policing has been implemented through cyber patrols, monitoring of strategic issues, analysis of digital conversations, and the issuance of early warnings to accounts with the potential to spread hate speech. Yet implementation remains suboptimal since policy communication lacks uniformity staffing and funding are constrained organizational readiness for data-driven methods is incomplete and analytical systems and procedures lack proper integration. In terms of competencies, personnel possess basic skills in cyber investigation and open-source intelligence (OSINT), but advanced competencies in predictive analytics, artificial intelligence (AI), big data analytics, machine learning, and natural language processing remain limited and are not evenly distributed across all units. This situation is influenced by the lack of competency standards specifically designed to support the implementation of predictive policing. This research strengthens data-driven policing in Indonesia via competency standards, analytics systems, and workforce development supporting predictive policing against hate speech.

Keywords: Competency, Hate Speech, Predictive Policing, Pre-Emptive, Social Media.

1. Introduction

Information technology has opened a new space for the public to express opinions, engage in discussions, and interact, one of which is through social media. Social media not only functions as a means of communication and information exchange, but has also developed into a medium for commerce, dissemination of government policies, political campaigns, and religious outreach (Buntoro, 2016). However, this development has also been accompanied by the emergence of various forms of cybercrime, one of which is hate speech.

Hate speech on social media involves communication that targets specific individuals or groups with elements of hatred, potentially causing harm to those affected (Patihullah & Winarko, 2019). It can take the form of incitement, insults, or demeaning actions based on religion, race, ethnicity, gender, or other identities (Putra & Nurjanah, 2020). In its development, hate speech in Indonesia has shown a significant increase in line with the growing intensity of social media use, which has also facilitated the spread of social conflict.



Data from the Ministry of Communication and Information Technology shows that content containing hate speech that was acted upon in 2023 increased, accompanied by the blocking of thousands of social media accounts that violated SARA (ethnicity, religion, race, and inter-group) provisions (Nidhal et al., 2025). This phenomenon is reinforced by research from Monash University and AJI Indonesia, which recorded 182,118 posts containing hate speech during the 2024 Election period, with dominance on the platforms X/Twitter, Facebook, and Instagram (Monash University, 2025). The most dominant types of hate speech were identity-based attacks, followed by insults, obscenities, threats, and sexual speech (Monash University, 2025).

The impact of hate speech is not only individual but also has implications for social and political stability. The study by Pérez-Escolar and Noguera-Vivo (2021) shows that online hate speech can trigger polarization, reinforce fanaticism, and damage the public discourse space. In Indonesia, hate speech has also frequently become a trigger for social conflict and a tool of political propaganda (Hutabarat & Radhiah, 2025). In addition, Dreißigacker et al. (2024) reveal that victims of hate speech experience psychological impacts in the form of anxiety, depression, and a decline in their sense of security and trust in institutions.

Normatively, Indonesia has regulated the prohibition of hate speech through Article 28 paragraph (2) of the Law on Electronic Information and Transactions (UU ITE) and the Chief of Police Circular Letter Number SE/6/X/2015. However, the implementation of these regulations still faces challenges, particularly regarding the boundary between freedom of expression and hate speech, as well as the potential for legal misuse (Yolanda, 2021). On the other hand, technological limitations in monitoring the massively growing digital content also constitute an obstacle in law enforcement (Lahinda et al., 2025).

Based on data from the Cyber Directorate of Bareskrim Polri, hate speech cases fluctuated during 2019 to 2025, with dominance in the forms of defamation, SARA, and threats. In addition, there is a gap between the total number of cases (Crime Total) and their resolution (Crime Clearance) in certain periods, indicating the complexity of handling cases in the digital realm. This condition shows that hate speech is rapidly evolving, cross-platform in nature, and difficult to control through conventional approaches.

Conventional approaches to handling hate speech have various limitations, including slow response, subjectivity in the interpretation of law enforcement officers, and limited resources for conducting massive monitoring (Grattet & Jenness, 2005). Perpetrators can also easily evade detection through the use of coded language or account switching (Shuy, 2005). Furthermore, social media algorithms still have limitations in understanding language context, particularly in the form of sarcasm or local language variations (MacAvaney et al., 2019; Vidgen et al., 2020).

These conditions have driven the development of the predictive policing approach as an alternative in technology-based law enforcement. Predictive policing utilizes historical data and analytics to predict the potential for crime and support prevention efforts (Hamid, Syafruddin, & Lubis, 2023; Camacho-Collados & Liberatore, 2015; Norton, 2013). This approach has also been supported by the development of big data and artificial intelligence in crime pattern analysis (Egbert & Krasmann, 2019; Tatikonda & Ganguli, 2025).

However, the effectiveness of predictive policing is determined not only by the availability of technological infrastructure and analytical systems, but also by the competence of the personnel responsible for operating, interpreting and utilising the predictive results. Advanced technologies such as artificial intelligence and big data analytics require adequately trained staff to ensure that predictive information can be translated into sound operational

decisions. Consequently, staff competence is an integral component of the successful implementation of predictive policing, rather than merely a separate organisational issue.

In several countries, predictive policing has been applied to monitor hate speech digitally, including the use of AI and natural language processing (Chen et al., 2003; Schmidt & Wiegand, 2017). In Indonesia, this approach has begun to be adopted in data-based policing systems; however, its implementation is still partial and has not yet been optimally integrated (Wibowo et al., 2023). In addition, there are obstacles in the form of misconceptions about the concept, limitations of data management units, and suboptimal evaluation of the system (Sumirat et al., 2021).

Another problem lies in human resource competency. Digital transformation in law enforcement demands adequate data analysis capabilities and technology mastery (Chan, 2001; Manning, 2022). However, the Cyber Crime Directorate of Bareskrim Polri, with its limited personnel, still faces competency limitations in the areas of artificial intelligence and big data analytics due to insufficient training and budget constraints. Many personnel do not yet hold specialized certifications in the cyber field, so the implementation of predictive policing has not yet run optimally (Tambunan, 2023).

Based on the foregoing background, the main problem in this study can be formulated around how the implementation of predictive policing as a form of the pre-emptive function in combating the spread of hate speech on social media is carried out by the Cyber Crime Directorate of Bareskrim Polri, and how the competencies of the human resources it possesses support the implementation of this approach. This problem arises because the increasing spread of hate speech on social media is not proportional to the effectiveness of conventional approaches in handling it, as well as the limited integration of technology and human resource capacity in supporting data-based policing.

Existing research on hate speech in Indonesia has largely focused on the normative legal framework, legal analysis of the Law on Information and Electronic Transactions (ITE Law), and reactive law enforcement approaches. Relatively few studies have empirically examined how predictive policing is applied in operational practice, particularly regarding the integration of artificial intelligence, data analytics, and human resource competencies within the Cybercrime Directorate of the Indonesian National Police's Criminal Investigation Agency (Bareskrim). As the effectiveness of predictive policing depends on both technological capabilities and the competencies of the personnel responsible for operating predictive systems, this study addresses this gap by examining both dimensions simultaneously. Consequently, the uniqueness of this research lies in the integration of technological, organisational and human resource perspectives to provide an empirical evaluation of predictive policing in combating hate speech on social media within the Cybercrime Directorate of the Indonesian National Police's Criminal Investigation Agency (Bareskrim).

2. Literature Review

2.1. Predictive Policing

According to Tayebi and Glasser (2016), predictive policing is a multidisciplinary policing strategy based on advanced analytics to build crime prevention mechanisms, while Meijer and Wessels (2019) emphasize that this approach focuses on collecting and analyzing historical data in order to predict individuals or areas with a higher probability of crime. This approach encompasses four main dimensions, namely the prediction of offenders, victims, criminal collaboration, and crime location, each of which employs techniques such as

historical data analysis, machine learning, Social Network Analysis, data mining, hotspot mapping, and Geographic Information Systems (GIS).

2.2. Pre-emptive

The term pre-emptive generally carries the meaning of preventing or anticipating the occurrence of something before the event actually takes place (Bunn, 2003). In the context of law and security, this concept developed rapidly following the September 11, 2001 attacks in the United States, when pre-emptive efforts began to be incorporated as part of national security strategy to respond to threats that are unpredictable and potentially capable of causing great harm (Sofaer, 2003). This approach emphasizes actions taken against threats that are anticipated to occur imminently, even when certainty is not yet fully established, making it more anticipatory in nature and based on presumptions or possibilities of future risk (Egbert & Krasmann, 2019). From a legal perspective, pre-emptive action is understood as an early detection effort directed at criminogenic factors that can trigger criminal acts, thereby enabling prevention before crime actually emerges (Siahaan, 2004).

2.3. Hate Speech

Hate speech is an oral or written statement in the public sphere that aims to incite hatred, hostility, or discrimination against individuals or groups based on race, religion, ethnicity, gender, disability, or sexual orientation (Carlson, 2021). In law, such speech encompasses actions such as insult, defamation, blasphemy, incitement, provocation, and the spread of false information that can trigger social conflict (Anam & Hafiz, 2015; Soesilo, 1995). Hate speech also targets vulnerable groups and can be disseminated through various media such as social media, campaigns, pamphlets, lectures, and mass media, thereby having the potential to cause discrimination and disruption of social order (Gagliardone et al., 2015).

2.4. George Edward III's Implementation Theory

Implementation Theory by George Edward III describes policy implementation as the execution of decisions or programs to meet set objectives (Usman, 2002; Wahab, 2021). The effectiveness of this process hinges on four key factors: communication, resources, disposition, and bureaucratic structure (Widodo, 2007). These components are interconnected in influencing how effectively policies are carried out, and a breakdown in any one can lead to implementation failure.

2.5. Routine Activity Theory

Routine Activity Theory explains that crime occurs due to the convergence of three main elements, namely a motivated offender, a suitable target, and the absence of a capable guardian (Cohen & Felson, 1979). This theory emphasizes that crime is not only influenced by the offender's intent, but also by the conditions of daily activities and social situations that enable crime to occur. In the modern context, changes in activity patterns, including in the digital space, also influence the emergence of criminal opportunities such as hate speech.

3. Methods

This study uses a qualitative method with a phenomenological approach to understand the implementation of predictive policing in preventing hate speech on social media by the Cyber Crime Directorate of Bareskrim Polri. The phenomenological approach is used to explore the subjective experiences of law enforcement officers in the execution of this policy, thereby obtaining a deep understanding of field practices. Research data sources consist of primary data in the form of in-depth interviews with law enforcement officers and secondary

data encompassing scientific journals, academic books, articles, and related policy documents and regulations. Data collection techniques were carried out through interviews and documentation selected purposively in accordance with their relevance to the research focus.

Data analysis used content analysis with the stages of data reduction, categorization, and interpretation to discover patterns and meanings from the data obtained. This process follows the Miles and Huberman model, which encompasses data reduction, data presentation, and conclusion drawing. Data validity was assessed through source triangulation by comparing information obtained from various documents, such as legislation, official reports and relevant academic literature. Further, this study utilises Edward III's policy implementation framework as the primary basis for analysing the data, supported by Routine Activity Theory to explain specific aspects relating to the occurrence of criminal offences in the digital sphere. This approach aims to enhance the validity and depth of the research analysis.

4. Results and Discussion

4.1. Implementation of the Predictive Policing Approach as a Form of the Pre-emptive Function Against the Spread of Hate Speech on Indonesian Social Media by the Cyber Crime Directorate of Bareskrim Polri

Hate speech crime cases on Indonesian social media show a declining trend, as illuminated in table 1.

Table 1. Total Hate Speech Crime Cases in Indonesia, 2019 to 2025

Type of Hate Speech	2019	2020	2021	2022	2023	2024	2025
Hoax/Fake News	37	36	12	9	6	7	3
Defamation	53	55	15	32	11	13	16
Hate Speech/SARA	22	6	21	8	9	4	6
Threats	7	5	11	5	5	3	3
Total	119	102	59	54	31	27	28

Source: Cyber Directorate of Bareskrim Polri (2025)

According to Table 1, the number of hate speech criminal cases handled by the Cybercrime Directorate (Ditpid Siber) of the Indonesian National Police's Criminal Investigation Agency (Bareskrim) during the period 2019–2025 shows a downward trend. However, the decrease in the number of cases prosecuted does not necessarily indicate a reduction in the practice of hate speech on social media. This discrepancy indicates a gap between the number of cases successfully handled by law enforcement agencies and the actual incidence of hate speech occurring in the digital sphere. This situation suggests that hate speech is becoming increasingly complex and difficult to detect, thereby necessitating more effective monitoring and law enforcement mechanisms.

Table 2. Comparison of Types of Hate Speech Before and After the 2024 Election

No.	Types and Quantities of Hate Speech Before the 2024 Election	Platform	Types and Quantities of Hate Speech After the 2024 Election	Platform
1	Identity attacks (SARA) (123,968 contents)	1. Twitter (51.2%) 2. Facebook (45.15%)	Hoaxes (1,674 contents)	1. TikTok 2. Twitter (51.2%) 3. Facebook (45.15%)

No.	Types and Quantities of Hate Speech Before the 2024 Election	Platform	Types and Quantities of Hate Speech After the 2024 Election	Platform
2	Insults (104,664 contents)	3. Instagram (3.34%)	Provocation/incitement (592 contents) (Martiar, 2025)	4. Instagram (3.34%)
3	Obscenities (42,267 contents)		Defamation	
4	Threats (39,153 contents)		Threats	
5	Sexual/vulgar content (3,528 contents)			
6	Hoax/fake news (2,330 contents)			

Source: Researcher's processed data

The data clearly shows that hate speech cases on social media are most prevalent during certain periods, such as the period leading up to elections, because even after the election is concluded, those hate speech cases also decline. With the increase in hate speech cases and the many impacts caused by such actions, handling hate speech, particularly prevention efforts, is very important so that hate speech does not spread widely. In this regard, Brigadier Police Officer Irfan Hasi Sagala, Bhaops Unit V Subdit III Dittipidsiber, stated that *"Handling is carried out preventively, pre-emptively, and repressively through education, cyber patrols, and law enforcement."*

In the digital era, pre-emptive efforts can be carried out by utilizing developing digital technologies to make predictions with the aim of preventing harmful actions (crimes) from occurring, or what is known as predictive policing, as stated by Van Brakel (2025) that the pre-emptive logic can be recognized in many new surveillance practices, such as predictive policing. As said by Moses and Chan (2018), conceptually, predictive policing shares similarities with but is distinct from various law enforcement strategies such as intelligence-led policing (ILP), data-driven policing, risk-based policing, hotspot policing, evidence-based policing, and preventive policing. When considering pre-emptive action, the distinction between pre-emptive and predictive policing is that pre-emptive policing does not always rely on data-driven predictions. Consequently, pre-emptive measures fall short in addressing cybercriminals who take advantage of the vast and interconnected nature of social media.

Moreover, the pre-emptive efforts carried out by Polri are limited to providing digital literacy education to the public. Meanwhile, hate speech actions on social media involve an extremely large number of content uploads every day. This is obviously not sufficient to prevent the spread of hate speech on social media. Thus, the use of the predictive policing approach can become an alternative to maximize the pre-emptive efforts that have already been undertaken.

The virtual police is essentially a police unit program formed under Bareskrim Polri with the aim of protecting the public from various types of cybercrime, particularly the spread of disinformation and hate speech (Sardini, Wijayanto, & Elsitra, 2024). The virtual police is tasked with educating the public so that they do not spread content laden with legal violations and susceptible to the UU ITE. Sari (2021) explains that in carrying out their duties, police officers serving as virtual police will conduct surveillance of social media accounts. When an account is found to have uploaded text or images with the potential to violate the law, the

officer will save a screenshot of the upload to be consulted with an expert team consisting of criminal law experts, language experts, and electronic information and transactions experts. If the expert determines that the content contains a criminal violation, the next step is to submit it to the cyber director or the designated cyber official for approval. They will then send a warning to the social media account suspected of committing the violation directly and officially to the account in question. The warning will be sent via direct message, as the police do not want the virtual police warning to the social media user to be known by other parties, because it is confidential in nature.

In practice, the cyber patrol efforts carried out by Bareskrim Polri are based on the results of data analysis, particularly historical data on previous hate speech cases, to map trends in patterns, timing, and actors suspected of having previously spread hate speech. The data used as analytical material comes from two sources, as revealed by the Cyber Sub-Unit Head, Police Commissioner Firdaus, S.H., as follows:

"In conducting analysis and predictions, we use various data sources, both internal and external. From the external side, the main sources come from social media platforms such as Twitter/X, Facebook, and Instagram. In addition, public reports also serve as an important source that provides initial information regarding the existence of problematic content. From the internal side, we utilize data from previous cases as a reference to identify recurring patterns. Furthermore, the results of cyber patrols also serve as a primary data source that is continuously updated in real time. We also coordinate with other agencies such as Kominfo to obtain additional relevant data."

Furthermore, Brigadier Police Officer Irfan Hasi Sagala, Bhaops Unit V Subdit III Dittipidsiber, stated that *"the implementation of predictive policing to prevent the spread of hate speech is supported by the use of monitoring tools and sentiment analysis."* Similarly, Brigadier Police Officer Anuar, Ba Unit V Subdit III Dittipidsiber, stated that:

"I use software (both developed internally and in collaboration with third parties) that utilizes Big Data Analytics and artificial intelligence (AI) to carry out crawling (automated data collection), Social Network Analysis (SNA), and Sentiment Analysis from various social media platforms."

In contrast to these two members of Dittipidsiber Bareskrim Polri, the Cyber Sub-Unit Head, Police Commissioner Firdaus, S.H., provided a different explanation regarding the use of predictive technology at Bareskrim Polri as follows:

"The predictive technology used in implementing predictive policing is still limited to a combination of digital tools and manual analysis by personnel, because we are currently still in the development stage and have not yet been fully optimal. There have indeed been efforts directed toward the use of such technology, but its implementation has not yet been fully integrated into a single solid national system."

The results of the interviews with these three respondents show that Bareskrim Polri itself has not yet fully employed digital predictive technologies in implementing predictive policing, such as AI, big data analytics, and others. Yet the use of such technologies is very important to maximize the effectiveness and benefits of implementing predictive policing.

Research findings show that the implementation of predictive policing at the Cyber Crime Directorate of Bareskrim Polri still faces technological and data integration limitations. Yet various studies have shown that the utilization of big data analytics and artificial intelligence can improve the capability for early detection, risk mapping, and the effectiveness

of resource allocation in crime prevention efforts (Ali et al., 2025; Meijer & Wessels, 2019; Perry et al., 2013). Therefore, strengthening digital infrastructure and analytical systems is an important factor in supporting the effectiveness of predictive policing.

Brigadier Police Officer Irfan Hasi Sagala, Bhaops Unit V Subdit III Dittipidsiber, stated that *“in terms of the success of the predictive approach, Polri has successfully prevented provocative narratives through early detection and counter-narratives.”* Brigadier Police Officer Anuar, Ba Unit V Subdit III Dittipidsiber, then further elaborated that:

“During a large demonstration, the analytical system detected a network of bot (automated) accounts that began pushing provocative hashtags and hoaxes about ‘security forces attacking religious figures.’ Before the hashtag could become a Trending Topic and trigger mass unrest in the real world, the Cyber team mapped the main actors, coordinated with Kominfo to take down the hoax content, and simultaneously the Public Relations Division released a video clarifying the actual facts on the ground. Offline conflict was successfully prevented.”

In addition, Police Commissioner Firdaus, S.H., Cyber Sub-Unit Head, stated that:

“To predict areas, groups, and periods prone to hate speech, Polri uses an AI-based system and big data analytics. Although still in the development stage and not yet fully optimal, the system is quite helpful in detecting hate speech that is explicit in nature, such as direct insults or clearly SARA-based speech.”

This statement implies that predictive policing is essentially quite effective in preventing the occurrence of hate speech dissemination based on the results of data analysis collected from hate speech content uploaded on social media.

Nevertheless, its effectiveness is still not at its maximum, given that there are still many factors that hinder it. In this regard, implementation in theory refers to a method carried out so that a particular policy can achieve its goals, as stated by Alizah and Mawar (2024) that the implementation process will only begin when goals and targets have been set, activity programs have been arranged, and funding has been prepared and channeled to achieve the targets (Alizah & Mawar, 2024). According to Edward, policy implementation is influenced by several factors below.

4.1.1. Communication

In this regard, Brigadier Police Officer Irfan Hasi Sagala, Bhaops Unit V Subdit III Dittipidsiber, stated that predictive policing has begun to be implemented but has not yet been fully formalized. He also added that the predictive policing policy has been communicated but has not yet been evenly distributed. Brigadier Police Officer Anuar, Ba Unit V Subdit III Dittipidsiber, then added that this policy has been communicated hierarchically through Telegram Letters (TR), leadership directives, and various Technical Guidance (Bimtek) sessions. Furthermore, Police Commissioner Firdaus, S.H., Cyber Sub-Unit Head, provided the following explanation:

“Normatively, there is indeed no policy document that explicitly mentions the term ‘predictive policing’ as a formally adopted concept by the Cyber Directorate. Nevertheless, regarding policy communication, the policy direction oriented toward data-based policing has essentially been conveyed through various internal forums, both in the form of leadership directives, analysis and evaluation forums, and other technical activities.”

Based on the results of these interviews, it can be understood that the predictive policing policy for the purpose of preventing the spread of hate speech on social media has essentially

been communicated by Bareskrim Polri to all members of Polri, particularly Dittipidsiber. Unfortunately, these communication efforts are still not evenly distributed, meaning that not all members of Polri are aware of this policy. In addition, the clarity of the delivery of the predictive policing policy message is also still lacking, as expressed by Brigadier Police Officer Anuar, Ba Unit V Subdit III Dittipidsiber, that “... *the level of technical understanding in the field can vary between personnel at Mabes Polri and those at the regional or district police level.*” Similarly, Police Commissioner Firdaus, S.H., Cyber Sub-Unit Head, provided the following explanation:

“...Regarding policy communication, in principle, the policy direction for strengthening the data-based approach has often been conveyed by leadership, both through official forums such as analysis and evaluation (anev) sessions, coordination meetings, and internal briefings. However, in its implementation, understanding of this concept has not yet been fully distributed among all members. There are still differences in perspective between members who already have exposure to technology and data analysis and members who are still accustomed to the conventional, more reactive approach. This is influenced by the educational background, experience, and level of technological literacy of each personnel.”

4.1.2. Resources

In relation to the implementation of predictive policing as a pre-emptive effort against the spread of hate speech on social media, in terms of human resources, Brigadier Police Officer Irfan Hasi Sagala, Bhaops Unit V Subdit III Dittipidsiber, stated that the competencies available for conducting predictive policing are sufficient, but predictive analytics need to be improved. Brigadier Police Officer Anuar, Ba Unit V Subdit III Dittipidsiber, also provided a similar statement that the majority of investigators have a basic understanding of digital behavior and OSINT. However, specific competencies for advanced data mining and predictive analytics are generally possessed only by specialized personnel (data analysts) in certain units, and have not yet been evenly distributed to all field members. Furthermore, Police Commissioner Firdaus, S.H., Cyber Sub-Unit Head, provided the following explanation:

“Human resource limitations are one of the most significant constraints. In terms of quantity, the number of available personnel is actually limited compared to the workload that must be handled, especially in facing the enormous volume of activity on social media. In terms of quality, some personnel do have basic understanding related to cybercrime, but for more specific competencies such as predictive analytics, data mining, big data analytics, and understanding of digital behavior, these still need to be improved systematically. There is also a challenge in terms of mindset, where not all personnel are accustomed to working with a data-based approach, so it requires an adaptation process that is not short. Furthermore, in terms of human resources, not all personnel are yet able to use technology in a proper and proficient manner; in addition, the UU ITE still requires interpretation to be provided by our own personnel, so whether something can be classified as hate speech is a subjective interpretation that varies among our members; moreover, some of our personnel are already of quite an advanced age, so their use of technology is still very limited.”

Then, regarding the financial resources aspect, Police Commissioner Firdaus, S.H., Cyber Sub-Unit Head, stated in his interview that:

“From the budget aspect, one of the main constraints is the limitation of allocation specifically designated for the development of analytical technology and big data-based systems. The development of a predictive policing system requires considerable investment, both for technological infrastructure, the procurement of sophisticated software, and the continuous maintenance of such systems. Meanwhile, other operational needs that are also

of priority nature often mean that budget allocations must be divided, so that the development of predictive systems cannot yet be carried out optimally and comprehensively.”

Lastly, regarding infrastructure resources, Police Commissioner Firdaus, S.H., Cyber Sub-Unit Head, stated that:

“From the aspect of facilities and technological infrastructure, we currently already have several devices and applications that support cyber patrol activities and social media monitoring. However, these systems are still partial in nature and have not yet been integrated into a single national platform capable of processing data comprehensively. Ideally, predictive policing requires a big data system capable of combining various data sources, performing analysis automatically, and producing outputs in the form of predictions that can be used as the basis for decision-making. Current conditions indicate that we are still moving in that direction, but have not yet reached the expected level of integration.”

These statements indicate that the implementation of predictive policing by Dittipidsiber Bareskrim Polri in preventing the spread of hate speech on social media is still not supported by adequate resource availability, whether in terms of human resources, budget, or supporting infrastructure.

4.1.3. Disposition

Disposition is a factor relating to the attitudes, commitment and willingness of policy implementers to put a policy into practice. According to Edward III (Mubarok et al., 2020), disposition reflects the willingness, commitment and dedication of implementers to carry out the policy in accordance with the established objectives. Policy implementation depends not only on the technical capabilities and understanding of those responsible for implementation, but also on a strong commitment to carrying out the policy consistently and effectively (Mubarok et al., 2020).

In the implementation of predictive policing as a pre-emptive measure against the spread of hate speech on social media, interview findings indicate that personnel from the Cybercrime Directorate (Dittipidsiber) of the National Police’s Criminal Investigation Agency (Bareskrim) fundamentally possess the willingness to implement this approach. Police Brigadier Irfan Hasi Sagala, of the Operations Unit V, Sub-Directorate III, Dittipidsiber, stated that “in general, we are ready, but our analytical and technological capabilities still need to be improved.” This statement indicates that the implementers are committed to applying predictive policing, whilst acknowledging that there are still capacity limitations that need to be addressed.

This commitment is also reflected in the statement by Police Brigadier Anuar, Head of Unit V, Sub-Directorate III of the Cybercrime Directorate, who explained that the majority of investigators already possess a basic understanding of digital behaviour and Open Source Intelligence (OSINT), and have utilised software based on Big Data Analytics and Artificial Intelligence (AI) to carry out crawling, Social Network Analysis (SNA) and Sentiment Analysis on various social media platforms. This demonstrates the organisation’s willingness to adopt technology as part of the transformation of law enforcement methods.

However, the research findings also indicate a discrepancy between the level of readiness reflected in individual commitment and the organisation’s overall readiness. The Head of the Cyber Sub-Unit, Police Commissioner Firdaus, S.H., explained that the Cyber Crime Investigation Directorate (Dittipidsiber) of the Indonesian National Police’s Criminal

Investigation Agency (Bareskrim) is not yet fully prepared to implement predictive policing, particularly in making the transition from a reactive approach to a data-driven policing approach. These findings suggest that implementation challenges are not solely due to variations in individual readiness, but also reflect organisational challenges in managing change.

From an organisational change management perspective, the transformation towards predictive policing requires a shift in work culture, the strengthening of human resource capacity, and the adaptation of work systems to support data-driven decision-making. Thus, although staff motivation and willingness are relatively high, implementation cannot proceed optimally unless accompanied by organisational support in the form of skills development, the provision of technological infrastructure, and coordination and evaluation mechanisms that support this change process.

These findings are also consistent with the concept of Public Service Motivation (PSM), which explains that civil servants' intrinsic motivation to provide public services is a vital asset in policy implementation. However, this motivation needs to be supported by a conducive organisational environment in order to be realised in the form of optimal performance. Hence, the disposition of the implementers in this study can be assessed positively, as there is a strong willingness and commitment to implement predictive policing. However, the effectiveness of its implementation is still influenced by the organisation's readiness to manage the transition towards a more predictive and data-driven law enforcement system.

4.1.4. Bureaucratic Structure

Bureaucratic structure is an organizational design in which managers allocate the resources possessed by the organization, particularly those related to the division of labor and the resources owned by the organization, as well as how the overall work can be coordinated and communicated (Sule & Saefullah, 2005). Hasibuan (2017) states that bureaucratic structure is a depiction of the type of organization, departmentalization of the organization, positions and types of authority of officials, fields and work relationships, command lines and responsibilities, span of control, and the leadership system of the organization. Therefore, it can be said that organizational structure is a framework focused on the differentiation of positions, formulation of rules, procedures, and authority.

Bureaucratic structure is very important for the sustainability of an organization in achieving its established goals, as stated by Agustino (2006) that bureaucratic structure influences the success of policy implementation. Even when resources for implementing the policy are available and the implementers also know what needs to be done, implementation may be hindered because of weaknesses in the bureaucratic structure (Agustino, 2006). Two characteristics that must be considered in evaluating bureaucratic structure are the SOPs present in the organization and the fragmentation that exists in the execution of tasks. Fragmentation refers to the spread of responsibility for a policy across multiple entities, necessitating coordination in its execution. Such a fragmented bureaucratic framework can heighten the risk of communication breakdowns due to significant information distortion. As information becomes more distorted, the need for intensive coordination increases. Even with sufficient resources and knowledgeable, willing implementers, ineffective bureaucratic structures can hinder successful policy implementation. This issue involves various aspects, including the bureaucratic framework, authority distribution, and inter-unit relationships (Mubarak et al., 2020).

In relation to the implementation of predictive policing as a pre-emptive effort against the spread of hate speech on social media, in terms of human resources, Brigadier Police Officer Irfan Hasi Sagala, Bhaops Unit V Subdit III Dittipidsiber, stated that predictive

policing is performed by involving coordination with intelligence, analysis, and cyber patrol functions.

The results of the interview show that the bureaucratic structure in the implementation of predictive policing is already sufficiently fragmented, with each implementing unit having its own tasks and responsibilities while being complementary to one another. The structure formed is also not deeply layered, so that coordination can be carried out effectively. However, because the SOPs are too complex, coordination efforts in the implementation of predictive policing are often hindered because approval must be awaited. Furthermore, Polri also still faces the constraint of integrating the application systems it uses, including in the execution of coordination.

The findings from interviews concerning the implementation of predictive policing to prevent the spread of hate speech on social media align with the research by Berk (2021), which identifies several obstacles to predictive policing. These challenges include: 1) insufficient understanding of predictive policing concepts, as some Polri personnel lack the necessary comprehension of its fundamental principles, limiting their ability to apply its methods effectively; 2) inadequate skills in crime data analysis, with some personnel lacking proficiency in collecting, processing, and analyzing crime data, which hampers their ability to recognize crime patterns, evaluate risks, and implement suitable preventive actions; 3) limited training and educational resources, as access to training specifically focused on predictive policing is restricted, affecting personnel's ability to develop the needed skills and knowledge for effective use; 4) insufficient technological resources and infrastructure, since Polri doesn't possess all the technologies required for predictive policing, hindering efficient data processing and utilization; 5) weak collaboration and knowledge sharing, as there is a lack of cooperative efforts and knowledge exchange between Polri and academic, research, or governmental entities, which can stall the advancement of predictive policing and obstruct efforts to enhance personnel skills.

4.2. Human Resource Competency of the Cyber Crime Directorate of Bareskrim Polri in Implementing the Predictive Policing Approach as a Form of the Pre-emptive Function Against the Spread of Hate Speech on Indonesian Social Media

In his interview, Cyber Sub-Unit Head Police Commissioner Firdaus, S.H., stated that *"... Predictive policing demands high data analysis capabilities, an understanding of technologies such as artificial intelligence and machine learning, and the ability to read digital behavioral patterns..."* Brigadier Police Officer Irfan Hasi Sagala, Bhaops Unit V Subdit III Dittipidsiber, in his interview mentioned the competencies needed in predictive policing to prevent the spread of hate speech on social media as OSINT, digital forensics, network analysis, and machine learning. Furthermore, Brigadier Police Officer Anuar, Ba Unit V Subdit III Dittipidsiber, added that the competencies needed in predictive policing to prevent the spread of hate speech on social media are Social Network Analysis (SNA) for mapping the network of spreaders; Natural Language Processing (NLP) for filtering local language data; and Open Source Intelligence (OSINT) at an advanced level. Also needed is an understanding of sociology and digital psychology (understanding the psychological reasons why the public is easily provoked).

These statements imply that in order to implement predictive policing, law enforcement officers need special skills and competencies to be able to use the sophisticated technologies employed in predictive policing. In this regard, predictive policing is fundamentally not a new concept, but rather a continuation and transformation of traditional and analog policing practices with an increasingly expanding scale and shortened timeframe (Kaufmann et al.,

2019). The predictive policing model offers a new system that integrates technology to detect crime and then determine crime prevention measures (Sumirat et al., 2021). In its implementation, predictive policing centers on the capability of technology to drive the execution of pre-emptive actions by automating police decisions, so as to reduce overall crime harm by facilitating early intervention while also bringing efficiency benefits during periods of austerity (Sandhu & Fussey, 2021).

With the utilization of digital technology, law enforcement officers certainly need specialized competencies to implement it, particularly in relation to the use of digital technologies. Especially since although technologies such as AI and machine learning can assist in the implementation of early detection and crime prevention, the results of using such technology can easily generate false positives if information literacy and analytical skills are not strong, because these still require contextual interpretation of the results so that they can be transformed into valid and accurate intelligence data (Zakharevych & Hryhorenko, 2024). Therefore, specialized competency by the police, particularly in relation to the competency of technology use and predictive analytics, is an absolute necessity.

Furthermore, predictions regarding future criminal acts are also inseparable from strategic planning support. Like strategic planning in general, predictive policing is also part of a vision and a derivative of that overarching plan, meaning there is a series of follow-up actions as an elaboration of that vision and overarching plan. This series encompasses the determination of objectives, scope, delivery, milestones, resources, and action plans. In this context, in addition to building future predictions as previously mentioned, what is directly felt as a necessity is the execution of that series of follow-up actions. The internal side of predictive policing requires an organizational management system and physical and non-physical infrastructure, including personnel who possess the necessary competencies and skills. External needs include the development of relationships with data and information sources, knowledge, technology, and even funding (Seldadyo et al., 2022). Therefore, it can be said that the possession of competencies and skills, particularly those related to technology and predictive policing, is highly important and necessary.

In this regard, competency according to Sutton and Watson (2013) is a form of ability or expertise possessed by a person. Gunz (1983) defines competency as a person's underlying characteristic, which can be a motive, trait, aspect of a person's self-image or social role, or a body of knowledge that they use. This is consistent with what was stated by Mrowicki (1986) that competency is a description of the knowledge, skills, attitudes, and behaviors needed to perform real-life tasks. Similarly, Arifin (2021) defines competency as a set of personal and professional knowledge, skills, abilities, or attitudes for a particular task, job, or profession within the scope of job performance. In other words, competency is the integration of knowledge, skills, and abilities that leads to provable and measurable behavior as a manifestation of this competency.

This definition of competency shows that every task and job requires different competencies. This is because it is competency that will describe how people behave when they carry out their work. Thus, predictive policing and conventional policing possess and require different competencies, as stated by Sandhu and Fussey (2020) that the technology used in predictive policing requires support from the competencies possessed by police officers so that the prediction patterns generated become effective. In this regard, when an officer has unique expertise about a particular crime in their local jurisdiction, objective prediction errors caused by limited data or flawed calculations can be reduced by the opinion and subjectivity of police decisions (Sandhu & Fussey, 2020).

In connection with this, Craiger (2008) states that in this digital era, a competent police officer must be able to have technical understanding of various types of computer hardware, computer networks, operating systems, file systems, and various types of application software; an understanding of local, state, and federal laws that may apply during computer crime investigations; the ability to write detailed reports on the procedures used and the investigator's findings both technically and non-technically; and finally be able to accurately present evidence in court during criminal trials. In the context of predictive policing, the execution of predictive analytics techniques requires technical skill competencies, such as statistical analysis skills, statistical programming language skills, and data management skills (CNA, 2021).

The specific technical skill competencies required are based on several predictive policing techniques themselves, as can be seen in the following table (Carleton et al., 2020).

Table 3. Technical Skills for Predictive Analytics Techniques

Predictive Analytics Technique	Technical Skills
Hotspot detection	1. Use of general statistical analysis tools (e.g., Excel, GIS) 2. Programming skills 3. Ability to synthesize large amounts of data from various sources ranging from police reports to mapping and GIS data to recognize trends and patterns
Regression analysis	1. Use of statistical software packages and languages 2. Understanding of statistical concepts (e.g., probability, variance) and modeling 3. Ability to link multiple datasets
Targeted offender lists	1. Ability to link multiple datasets 2. Standardized approach to obtaining intelligence information from field officers, detectives, crime analysts, and other agencies 3. Understanding of crime patterns and gang institutionalization 4. Ability to synthesize large amounts of data from various sources (e.g., incident reports, CAD data, case files) to recognize trends and patterns
Risk terrain modeling (RTM)	1. Understanding of statistical concepts (e.g., probability) 2. Understanding of geospatial modeling, mapping, and coding 3. Use of GIS software
Machine learning algorithms	1. Understanding of statistical concepts (e.g., probability, variance analysis, hypothesis testing) and statistical modeling 2. Ability to link multiple datasets 3. Programming skills

Source: Carleton et al. (2020)

All of these competencies show that, just as the nature of policing continues to evolve, predictive analytics has also evolved in complexity and capability, from conventional predictive analytics, such as regression analysis, to more sophisticated statistical modeling, such as machine learning algorithms to predict crime and potential offenders and victims. In short, in predictive policing, law enforcement officers need advanced-level predictive analytics skills and competencies (Carleton et al., 2020). Without predictive analytics competency, the available technologies cannot be used and utilized to their maximum potential, and consequently the benefits provided by those technologies also cannot be maximized (Akdemir & Lawless, 2020).

In this regard, Fitzpatrick et al. (2019) describe predictive analytics in policing as using data to understand crime patterns over time and in different areas. This helps prevent crime and disorder. It builds on traditional crime analysis, which looks at crime trends and patterns. Predictive analytics not only identifies past trends but also predicts where and when crimes might happen and who might be involved. This gives police valuable information to better focus their efforts and use resources wisely, leading to more effective crime reduction and resource management.

The acquisition of advanced competencies in predictive analytics empowers law enforcement agencies to obtain valuable intelligence regarding criminal suspects, crime syndicates, and victims. An illustrative example is the Chicago Police Department, which leveraged predictive analytics to develop a Strategic Subject List (SSL). This list prioritized individuals with potential victimization risk alongside those with a heightened likelihood of engaging in violent behavior. The creation of the list was supported by software utilizing empirical data, which included factors such as the individual's criminal history, incidents of violence among their associates, the escalation of their criminal activities, and the severity of their past offenses (Ferguson, 2019). Similarly, in Kansas City, sophisticated social network analysis focused on potential crime perpetrators within the city was undertaken. A team from the Smart Policing Initiative (SPI) employed advanced network analysis technologies by utilizing violation records, gang-related information, and data from field interviews (Ferguson, 2019; Braga et al., 2014). This analytical approach facilitated the identification of socially deviant networks and the connections among deviant actors (Braga et al., 2014).

Therefore, this advanced predictive analytics competency is highly important and necessary for members of Dittipidsiber Bareskrim Polri to implement predictive policing in the context of preventing the spread of hate speech on social media. Especially since technology algorithms potentially experience problems, one of which is algorithmic bias. As has been stated, in algorithmic governance, as in the implementation of predictive policing, data has become the primary source of power. This data is collected from various sources. This is what often causes algorithmic bias to occur. This is because the formation and development of predictive model algorithms still requires experts, that is, humans, who are parties considered to be irrational and biased (Meijer et al., 2021; Peeters & Schuilenburg, 2023). Therefore, data collected by technology algorithms in the implementation of predictive policing also has the potential to contain bias.

The historical datasets underpinning predictive policing algorithms frequently mirror previous law enforcement practices, which may have been shaped by entrenched systemic racism, socioeconomic inequalities, and other forms of social injustice. Further, data collection methods tend to introduce bias, as they often depend solely on public service calls that may not truly capture the actual crime landscape within a community. Areas demonstrating greater community involvement might report higher crime rates, whereas less engaged neighborhoods may not attract the same level of scrutiny, thus skewing the data. Consequently, communities that have experienced historical inequities may be unjustly targeted, leading to a further deterioration of trust between law enforcement agencies and the community (Raji & Sholademi, 2024).

Thus, predictive analytics competency becomes one of the absolute competencies that must be possessed by the police to be able to implement predictive policing effectively. This is because a low level of this competency can give rise to the notion that every data generated by predictive technology is objective, when in fact such data often reflects over-policing in certain areas that is then replicated by the algorithm as a crime-prone area. As a result, they will continue to conduct over-policing in those areas as suggested by the technology algorithm

(Raji & Sholademi, 2024). In other words, predictive analytics competency can serve as a means of mitigating algorithmic bias in predictive policing, because with this competency, the police are able to test the algorithm for systematic errors and the data/information it produces.

Unfortunately, advanced predictive analytics competency is still not possessed by members of Dittipidsiber Bareskrim, as expressed by Brigadier Police Officer Anuar, Ba Unit V Subdit III Dittipidsiber, that specific competencies for advanced data mining and predictive analytics are generally possessed only by specialized personnel (data analysts) in certain units, and have not yet been evenly distributed to all field members.

The uneven distribution of competency possession is caused by the fact that Bareskrim Polri does not yet have established competency standards to support the implementation of predictive policing. Bryson and Daniels (2008) define competency standards as a collection of resources encompassing skills, actions, technology, or processes that can improve organizational performance. Houston and Howsam (1974) then explain that competency standards are a collection of knowledge, skills, and behaviors that a person needs to possess in order to carry out their duties effectively in a particular job or profession. These competencies include both technical and non-technical skills required to achieve optimal work outcomes. With competency standards in place, organizations can ensure that every individual possesses the capabilities appropriate to the demands of the work, thereby improving work efficiency and effectiveness.

Conversely, the absence of such competency standards certainly has an impact on the human resource management of Bareskrim Polri, including the possession of competencies needed to implement predictive policing. This is because the absence of competency standards will cause recruitment to become undirected, meaning that the selection and recruitment of prospective employees have the potential to not align with the required competencies. In relation to predictive policing, the absence of competency standards requiring knowledge of data science, algorithms, or social computing means that the recruitment process will continue to produce personnel with the same profile, namely investigators who may be competent in conventional policing mastery, but do not possess the competencies appropriate to predictive policing, such as big data analytics, AI, and so forth.

Furthermore, the absence of competency standards can also cause training programs to lose focus. In this case, the absence of such competency standards will cause training programs to lack curricula and training materials appropriate for developing predictive policing competencies. In other words, the absence of these competency standards will cause police officers to find it difficult to develop in accordance with the needs of predictive policing itself.

In his interview, Cyber Sub-Unit Head Police Commissioner Firdaus, S.H., also revealed that in order to implement predictive policing, law enforcement officers must also have the ability to act proactively. This is explained by Fitzpatrick et al. (2019) that incorporating predictive analytics into crime prevention signifies a shift towards proactive policing. This approach contrasts sharply with the conventional reactive method, which primarily focuses on responding to external triggers like 911 emergencies and citizen grievances or delving into the intricacies of active investigations. The core objective is to discern the recurring patterns or underlying causes leading to different crimes and then strategically allocate resources for focused interventions.

Bachner (2013) also states that the focus of predictive policing is proactive, meaning that from the outset law enforcement officers must be able to act actively so that crime can be prevented. However, Cyber Sub-Unit Head Police Commissioner Firdaus, S.H., also revealed that not all personnel have the readiness to shift to that mindset. There is still a tendency to rely on intuition or field experience alone, without being supported by strong data analysis.

This statement implies that law enforcement officers still do not yet have the ability to make the change, particularly regarding cultural change to support the implementation of predictive policing. Therefore, it is no surprise that the lack of ability to make the cultural change in the transition to a data-based approach has caused the implementation of predictive policing in preventing the spread of hate speech on social media to not be at its maximum potential.

5. Conclusion

This study shows that the Cybercrime Directorate of the Indonesian National Police's Criminal Investigation Agency (Bareskrim) has begun to adopt a predictive policing approach as part of its pre-emptive function in an effort to prevent the spread of hate speech on social media. This is implemented through cyber patrols, the monitoring of content and issues that could potentially lead to offences, and the issuing of warnings to accounts suspected of committing offences via the Virtual Police mechanism. Nevertheless, the research findings indicate that the application of predictive policing is still at the development stage and is not yet fully supported by an integrated predictive system. In practice, the identification and analysis processes still rely on a combination of digital tools and manual analysis by personnel.

This research also found that the implementation of predictive policing has not yet been optimal as it continues to face various obstacles, including those relating to communication, resources, personnel disposition and bureaucratic structure. In terms of human resources, expertise in the fields of data analytics, artificial intelligence and predictive analytics is not yet evenly distributed amongst all personnel, thereby affecting the effectiveness of its implementation. Therefore, there is a need to strengthen human resource capacity, develop more integrated systems, formulate clearer policies and operational standards, and improve technological infrastructure so that the implementation of predictive policing, as a pre-emptive measure in tackling hate speech on social media, can proceed more effectively.

6. References

- Agustino, L. (2006). *Politik & kebijakan publik*. AIPI Bandung.
- Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: a lifestyle routine activities approach. *Internet Research*, 30(6), 1665–1687. <https://doi.org/10.1108/intr-10-2019-0400>
- Ali, W., Rehman, T. U., & Saeed, A. (2025). Artificial Intelligence in crime prevention and detection: Enhancing predictive policing and public safety. *Advance Social Science Archive Journal*, 4(02), 1534–1543. <https://doi.org/10.5281/zenodo.17577464>
- Alizah, B., & Mawar, M. (2024). Implementasi Kebijakan Unit Layanan Disabilitas Bidang Ketenagakerjaan Di Dinas Tenaga Kerja Kabupaten Tangerang. *Petanda: Jurnal Ilmu Komunikasi Dan Humaniora*, 6(1), 78–87. <https://doi.org/10.32509/petanda.v6i1.3801>
- Anam, M. C., & Hafiz, M. (2015). Surat Edaran Kapolri Tentang Penanganan Ujaran Kebencian (Hate Speech) dalam Kerangka Hak Asasi Manusia. *Jurnal Keamanan Nasional*, 1(3). <https://doi.org/10.31599/jkn.v1i3.30>
- Arifin, M. A. (2021). Competence, Competency, and Competencies: A Misunderstanding in Theory and Practice for Future Reference. *International Journal of Academic Research in Business and Social Sciences*, 11(9). <https://doi.org/10.6007/ijarbss/v11-i9/11064>
- Bachner, J. (2013). *Predictive policing: preventing crime with data and analytics*. IBM Center for the Business of Government Washington, DC.
- Bennett Moses, L., & Chan, J. (2018). Algorithmic prediction in policing: assumptions, evaluation, and accountability. *Policing and Society*, 28(7), 806–822.

- <https://doi.org/10.1080/10439463.2016.1253695>
- Berk, R. A. (2021). Artificial intelligence, predictive policing, and risk assessment for law enforcement. *Annual Review of Criminology*, 4(1), 209–237. <https://doi.org/10.1146/annurev-criminol-051520-012342>
- Braga, A. A., Webster, D. W., White, M. D., & Saizow, H. (2014). SMART approaches to reducing gun violence. *Washington, DC: US Department of Justice*, 4.
- Bryson, J. R., & Daniels, P. W. (2008). Skills, expertise and innovation in the developing knowledge economy: the case of business and professional services. *International Journal of Services Technology and Management*, 9(3–4), 249–267. <https://doi.org/10.1504/IJSTM.2008.019706>
- Buntoro, G. A. (2016). Analisis Sentimen Hatespeech Pada Twitter Dengan Metode Naïve. *Jurnal Dinamika Informatika*, 5(October), 1–12.
- Carleton, B., Cunningham, B., & Thorkildsen, Z. (2020). *The use of predictive analytics in policing*. <https://apps.dtic.mil/sti/trecms/pdf/AD1145696.pdf>
- Carlson, C. R. (2021). *Hate Speech*. The MIT Press. <https://doi.org/10.7551/mitpress/12491.001.0001>
- Chan, J. B. L. (2001). The Technological Game: How information technology is transforming police practice. *Criminal Justice*, 1(2), 139–159. <https://doi.org/10.1177/1466802501001002001>
- Chen, H., Zeng, D., Atabakhsh, H., Wyzga, W., & Schroeder, J. (2003). COPLINK. *Communications of the ACM*, 46(1), 28–34. <https://doi.org/10.1145/602421.602441>
- CNA. (2021). *The Use of Predictive Analytics in Policing Bulletin* (p. 4). <https://www.cna.org/quick-looks/2021/The-Use-of-Predictive-Analytics-in-Policing-Bulletin.pdf>
- Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), 588. <https://doi.org/10.2307/2094589>
- Craigier, P. (2008). Training and Education in Digital Evidence. In *Handbook of Digital and Multimedia Forensic Evidence* (pp. 11–22). Humana Press. https://doi.org/10.1007/978-1-59745-577-0_2
- Dreißigacker, A., Müller, P., Isenhardt, A., & Schemmel, J. (2024). Online hate speech victimization: consequences for victims' feelings of insecurity. *Crime Science*, 13(1). <https://doi.org/10.1186/s40163-024-00204-y>
- Egbert, S., & Krasmann, S. (2019). Predictive policing: not yet, but soon preemptive? *Policing and Society*, 30(8), 905–919. <https://doi.org/10.1080/10439463.2019.1611821>
- Ferguson, A. G. (2019). Predictive Policing Theory. In *The Cambridge Handbook of Policing in the United States* (pp. 491–510). Cambridge University Press. <https://doi.org/10.1017/9781108354721.025>
- Fitzpatrick, D. J., Gorr, W. L., & Neill, D. B. (2019). Keeping Score: Predictive Analytics in Policing. *Annual Review of Criminology*, 2(1), 473–491. <https://doi.org/10.1146/annurev-criminol-011518-024534>
- Gagliardone, I., Gal, D., Alves, T., & Martinez, G. (2015). *Countering online hate speech*. Unesco Publishing.
- Grattet, R., & Jenness, V. (2005). The reconstitution of law in local settings: Agency discretion, ambiguity, and a surplus of law in the policing of hate crime. In *Law and Society Review* (Vol. 39, Issue 4, pp. 893–942). Cambridge University Press & Assessment. <https://doi.org/10.1111/j.1540-5893.2005.00248.x>
- Gunz, H. (1983). The competent manager: A model for effective performance, Richard E. Boyatzis, Wiley, New York, 1982. No. of pages: 308. ISBN 0–471–09031–X. Price £21.75 (U.S. \$29.50). *Strategic Management Journal*, 4(4), 385–387. <https://doi.org/10.1002/smj.4250040413>

- Hasibuan, M. S. P. (2017). *Manajemen Sumber Daya Manusia*. Bumi Aksara.
- Houston, W. R., & Howsam, R. B. (1974). CBTE: The ayes of Texas. *The Phi Delta Kappan*, 55(5), 299–303. <https://www.jstor.org/stable/20297552>
- Hutabarat, K. D., & Radhiah, R. (2025). Ujaran kebencian pada kolom komentar media sosial akun instagram Anies Baswedan. *Kande: Jurnal Ilmiah Pendidikan Bahasa Dan Sastra Indonesia*, 6(1), 69–78. <https://doi.org/10.29103/jk.v6i1.20689>
- Kaufmann, M., Egbert, S., & Leese, M. (2019). Predictive policing and the politics of patterns. *The British Journal of Criminology*, 59(3), 674–692. <https://doi.org/10.1093/bjc/azy060>
- Lahinda, A., Tangkawarow, I. R. H. T., & Moningkey, E. R. S. (2025). Deteksi Ujaran Kebencian Pada Media Sosial Terkait Pemilu 2024 Menggunakan Algoritma Naive Bayes. *Jurnal Minfo Polgan*, 14(2), 3140–3155. <https://doi.org/10.33395/jmp.v14i2.15665>
- MacAvaney, S., Yao, H.-R., Yang, E., Russell, K., Goharian, N., & Frieder, O. (2019). Hate speech detection: Challenges and solutions. *PLOS ONE*, 14(8), e0221152. <https://doi.org/10.1371/journal.pone.0221152>
- Manning, P. K. (2022). *The Technology of Policing*. New York University Press. <https://doi.org/10.18574/nyu/9780814764442.001.0001>
- Meijer, A., Lorenz, L., & Wessels, M. (2021). Algorithmization of Bureaucratic Organizations: Using a Practice Lens to Study How Context Shapes Predictive Policing Systems. *Public Administration Review*, 81(5), 837–846. <https://doi.org/10.1111/puar.13391>
- 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>
- Monash University. (2025). *Report on Hate Speech Monitoring in The 2024 Indonesia Regional Elections*. Monash University. <https://www.monash.edu/indonesia/news/report-on-hate-speech-monitoring-in-the-2024-indonesia-regional-elections>
- Mubarak, S., Zauhar, S., Setyowati, E., & Suryadi, S. (2020). Policy Implementation Analysis: Exploration of George Edward III, Marilee S Grindle, and Mazmanian and Sabatier Theories in the Policy Analysis Triangle Framework. *Journal of Public Administration Studies*, 005(01), 33–38. <https://doi.org/10.21776/ub.jpas.2020.005.01.7>
- Nidhal, M., Aaron, R. A., & Alfari, A. (2025). Shadows of Censorship: Indonesia's Content Moderation Policy Development. *Policy Brief*, 31, 1–22. <https://doi.org/10.35497/619819>
- Patihullah, J., & Winarko, E. (2019). Hate Speech Detection for Indonesia Tweets Using Word Embedding And Gated Recurrent Unit. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, 13(1), 43. <https://doi.org/10.22146/ijccs.40125>
- Peeters, R., & Schuilenburg, M. (2023). Algorithmic Governance: Technology, Knowledge and Power. In *The SAGE Handbook of Digital Society* (pp. 439–457). SAGE Publications Ltd. <https://doi.org/10.4135/9781529783193.n25>
- Pérez-Escobar, M., & Noguera-Vivo, J. M. (2021). *Hate speech and polarization in participatory society*. Routledge.
- Perry, W., McInnis, B., Price, C., Smith, S., & Hollywood, J. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. RAND Corporation. <https://doi.org/10.7249/rr233>
- Putra, I. G. M., & Nurjanah, D. (2020). Hate Speech Detection In Indonesian Language Instagram. In *2020 International Conference on Advanced Computer Science and Information Systems (ICACSIS)* (pp. 413–420). IEEE. <https://doi.org/10.1109/icacsis51025.2020.9263084>
- Raji, I., & Sholademi, D. B. (2024). Predictive policing: The role of AI in crime prevention. *International Journal of Computer Applications Technology and Research*, 13(10), 66–

78. <https://doi.org/10.7753/IJCATR1310.1006>
- Sandhu, A., & Fussey, P. (2021). The ‘uberization of policing’? How police negotiate and operationalise predictive policing technology. *Policing and Society*, 31(1), 66–81. <https://doi.org/10.1080/10439463.2020.1803315>
- Schmidt, A., & Wiegand, M. (2017). A Survey on Hate Speech Detection using Natural Language Processing. In *Proceedings of the Fifth International Workshop on Natural Language Processing for Social Media* (pp. 1–10). Association for Computational Linguistics. <https://doi.org/10.18653/v1/w17-1101>
- Seldadyo, H., Sudarto, E. R., & Sonta, A. (2022). Predictive Policing: Current and Future Policing. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*, 5(1), 3906–3913. <https://www.bircu-journal.com/index.php/birci/article/view/4076>
- Shuy, R. W. (2005). *Creating language crimes: How law enforcement uses (and misuses) language*. Oxford University Press.
- Siahaan, N. H. T. (2004). *Hukum lingkungan dan ekologi pembangunan*. Erlangga.
- Soesilo, R. (1995). *Kitab Undang-Undang Hukum Pidana (KUHP): Serta Komentar-Komentarnya Lengkap Pasal Demi Pasal*. Politeia.
- Sule, E. T., & Saefullah, K. (2005). *Pengantar Manajemen*. Jakarta: Kencana.
- Sumirat, J. R., AN, S. D., & Adhikara, R. (2021). The Contemporary Policing Concept: How Globalisation Affected the New Concept of Indonesian Policing on Predictive Policing of “Presisi.” *Journal of Innovation Research and Knowledge*, 1(6), 147–156. <https://doi.org/10.53625/jirk.v1i6.638>
- Sutton, A., & Watson, S. (2013). Can competencies at selection predict performance and development needs? *Journal of Management Development*, 32(9), 1023–1035. <https://doi.org/10.1108/jmd-02-2012-0032>
- Tambunan, D. A. (2023). *Pemolisian di Era Digital: Strategi dan Tantangan Polri dalam Implementasi SmartPolicing*. STIKA.
- Tatikonda, R., & Ganguli, R. (2025). Predictive Summary Model—a Domain-Guided Approach to Generate Informative Summaries. *Mining, Metallurgy & Exploration*, 42(5), 2781–2793. <https://doi.org/10.1007/s42461-025-01316-y>
- Usman, N. (2002). *Konteks implementasi berbasis Kurikulum*. Jakarta: Grasindo.
- Van Brakel, R. (2025). Pre-emptive big data surveillance and its (dis) empowering consequences: The case of predictive policing. In *Exploring the boundaries of big data* (pp. 117–142). Routledge.
- Vidgen, B., Hale, S. A., Guest, E., Margetts, H., Broniatowski, D., Waseem, Z., Botelho, A., Hall, M., & Tromble, R. (2020). Detecting East Asian Prejudice on Social Media. In *Proceedings of the Fourth Workshop on Online Abuse and Harms* (pp. 162–172). Association for Computational Linguistics. <https://doi.org/10.18653/v1/2020.alw-1.19>
- Wahab, S. A. (2021). *Analisis kebijakan: dari formulasi ke penyusunan model-model implementasi kebijakan publik*. Bumi Aksara.
- Wibowo, A., Wangsajaya, Y., & Surahmat, A. (2023). *Pemolisian Digital dengan Artificial Intelligence*. PT. RajaGrafindo Persada-Rajawali Pers.
- Widodo, J. (2007). *Analisis kebijakan publik: Konsep dan aplikasi*. Boymedia Publissing, Malang.
- Yolanda, N. (2021). Date of Hate in Social Media (Facebook) According to Law Number 19 of 2016 Concerning Electronic Information and Transactions. *Awang Long Law Review*, 3(2), 96–107. <https://doi.org/10.56301/awl.v3i2.130>
- Zakharevych, M., & Hryhorenko, V. (2024). Digital Competence and Digital Literacy of Higher Education Acquires. *Collection of Scientific Papers of Uman State Pedagogical University*, 1, 119–129. <https://doi.org/10.31499/2307-4906.1.2024.302215>