TRANSPUBLIKA
Precise. Resilience. Felicitous.

Policy, Law, Notary and Regulatory Issues
https://ojs.transpublika.com/index.php/POLRI
Online ISSN 2809-896X

https://doi.org/10.55047/polri.v4i3.1801

Original Article

Digital Literacy as an Action Plan to Prevent Online Fraud Using the Triangle Scheme in the Jurisdiction of Makassar Police Headquarters

Rinal Krishna Triananda[1*], Basir S.[2], Muhamad Erza Aminanto[3]

[1-3]Police Science Studies, School of Strategic and Global Studies, Universitas Indonesia, Depok, Indonesia
Email: [1)] rinalkrishna2021@gmail.com, [2)] basir@ui.ac.id, [3)] erza.aminanto@ui.ac.id

Received : 12 May - 2025
Accepted : 14 June - 2025
Published online : 20 June - 2025

Abstract

This research aims to evaluate the effectiveness of preventive strategies implemented by the Makassar Police Headquarters (Polrestabes) in handling triangle scheme online fraud, a form of cybercrime that is increasingly prevalent alongside the rise in online transaction activities among the public. A qualitative approach with case study methodology is used to examine in depth the digital literacy strategies initiated by Makassar Police Headquarters, including collaboration between internal functional units and synergy with external stakeholders. Research findings indicate that although institutional frameworks and legal regulations are available, the implementation of digital literacy programs still faces constraints including budget limitations, gaps in digital technology mastery, and suboptimal reach of educational programs to peripheral areas. SWOT analysis and application of social system theory, community policing, and digital literacy implementation models indicate the need for strengthening human resource capacity, diversifying socialization methods, and establishing cross-sector collaborative forums to strengthen the community's digital security ecosystem. This research recommends the formulation of strategic policies that integrate digital literacy with law enforcement based on the Information and Electronic Transaction Law, Criminal Code, as well as personal data protection and consumer protection regulations. With a comprehensive and sustainable approach, prevention of triangle scheme online fraud can be optimized as part of the national cyber security strategy.

Keywords: Digital Literacy, Online Fraud, Triangle Scheme, Police Strategy, Cybercrime.

1. Introduction

The digital era has caused significant transformation in the processes used by individuals in building social relationships and conveying messages among themselves through various forms of communication. Individuals build social relationships and convey messages through various forms of communication (Rumata, 2017), which are now increasingly facilitated by advances in information and communication technology (ICT) that enable access to information anytime and anywhere. In the era of globalization, information technology has facilitated society in accessing and disseminating information quickly and widely. This development has made Indonesian society increasingly active in using online media. The "Digital 2024: Indonesia" report notes that the average internet usage time in Indonesia reaches 7 hours 38 minutes per day, with 3 hours 11 minutes of that time used to access social media exceeding the global average. Social media is used not only for leisure time but also as a means of maintaining social relationships and following current issues. This

phenomenon reflects the enormous influence of social media in modern social life and contemporary human dependence on information and communication technology.

Advances in information and communication technology bring positive impacts in various aspects of life, but also give rise to new forms of crime such as cybercrime, namely criminal acts committed through computer networks or the internet, including online fraud, identity theft, malware distribution, and attacks on state information systems (Kasim, 2024). Cybercrime not only harms individuals and companies but also potentially threatens national security. In Indonesia, data from the Cyber Patrol Website shows that online fraud is the most dominant form of cybercrime with 14,495 reported cases, reflecting the high vulnerability of society in digital spaces and the need for serious attention from law enforcement officials, including in the Makassar Police Headquarters area.

The triangle scheme mode is one of the online fraud techniques that is rampant, especially with the high public interest in purchasing used cars online. In this mode, perpetrators act as fictitious intermediaries who deceive both sellers and buyers by directing transactions through third parties who cannot be directly verified. Victims are asked to transfer a sum of money to the perpetrator, who then disappears after receiving the funds, causing financial losses to both parties. The low level of digital literacy among the public is exploited by criminals, which not only causes economic impacts but also significant psychological and social impacts such as loss of trust in online transactions and deterioration of digital platform image. In Makassar City, despite a fairly high level of internet penetration, online fraud cases continue to increase. Makassar Police Headquarters even receives reports almost daily regarding triangle scheme-based fraud, reflecting residents' lack of understanding of types of cybercrime. This condition indicates that improving digital literacy and strict law enforcement are urgently needed to prevent the spread of such criminal modes (Guntik & Yustiawan, 2022).

Throughout 2024, the Criminal Investigation Unit (Satreskrim) of Makassar Police Headquarters received 376 reports related to online fraud crimes, with an average of 31 reports per month. This trend shows a significant increase, as reflected in the number of reports in the first quarter of 2025 (January–March) which reached 112 cases. The high number of reports reflects that online fraud is one of the consistent and concerning forms of criminality in the Makassar Police Headquarters jurisdiction. However, the repressive approach that has been applied so far has not shown optimal effectiveness, given that the case clearance rate is recorded at less than 10% of total reports. One of the main obstacles in handling these cases is the complexity of the modus operandi, particularly the triangle scheme mode, which involves perpetrators, victims, and third parties whose identities are misused without the knowledge of the concerned party.

Based on these facts, efforts to combat online fraud crimes cannot rely solely on repressive approaches but must be strengthened through preventive strategies that are holistic, structured, and collaborative. Improving digital literacy becomes a crucial component in prevention efforts, given that internet penetration in Indonesia has reached 78.19% of the population (APJII, 2023). In this context, the Indonesian National Police (Polri) has a strategic role in handling cybercrime, but its effectiveness is highly dependent on the active involvement of various stakeholders, including government institutions, private sector, non-governmental organizations, and community participation (Januri et al., 2022).

Digital literacy encompasses not only skills in operating technological devices but also understanding personal data protection, cyber risk identification, and ethics of interacting in digital spaces. Lack of such understanding opens gaps for potential exploitation and cyber-attacks (Rahman, 2024). However, to date, the Criminal Investigation Unit of Makassar Police

Headquarters has not implemented collaborative digital literacy socialization or education programs with stakeholders. The absence of such initiatives indicates the need for policy formulation that supports systematic and cross-sector digital literacy development as an integral part of the national strategy in combating increasingly complex cybercrime.

Based on data, Satreskrim Makassar Police Headquarters last conducted digital literacy activities in 2023, which was done individually through social media, namely Instagram through its official account @satreskrim.mks. These activities took the form of educational photo and video uploads aimed at increasing public awareness of digital crime modes. However, from 2024 to the present (almost half of 2025) there have been no similar activities, either online or offline. This condition indicates a gap in continuous programs that should be of serious concern, given the increasing vulnerability of society to crimes in digital spaces. Therefore, there needs to be initiative and commitment from Satreskrim Makassar Police Headquarters to build systematic, collaborative, and sustainable digital literacy strategies.

Based on the background outlined above, the author is motivated to conduct further studies on the steps taken by the Indonesian National Police, particularly within the jurisdiction of Makassar Police Headquarters, in facing the challenges of increasingly complex and evolving online fraud crimes. The complexity of modus operandi, particularly the triangle scheme mode that is difficult to uncover through repressive approaches, demands more comprehensive, targeted prevention strategies involving various parties. Thus, this study is directed to examine how prevention strategies implemented by Makassar Police Headquarters in handling online fraud cases with triangle scheme modes, prioritizing preventive approaches that involve inter-agency synergy and strengthening community roles.

Digital literacy can be defined as a person's competence in using Information and Communication Technology (ICT) effectively to evaluate, access, find, communicate, and create information and content by utilizing technical and cognitive skills. The purpose of digital literacy is to provide education and advocacy to internet users regarding various aspects of safe internet use, including protection of personal data, online security, and individual privacy. Digital literacy education is becoming increasingly important, especially in Indonesia, which is one of the countries with high risk levels for information security threats. Lack of understanding regarding digital security can make individuals and organizations vulnerable to cyber-attacks. Therefore, the utilization of information technology in digital literacy education plays an important role in building awareness and improving society's ability to maintain digital security and protect their personal data (Rahman, 2024).

Based on the problem formulation and research questions that have been established, this research aims to evaluate the effectiveness of various steps that have been implemented in improving digital literacy among the public in the Makassar Police Headquarters jurisdiction. Additionally, this research also aims to formulate strategic policy recommendations that can strengthen efforts to prevent online fraud, particularly those using triangle scheme modes, more effectively and sustainably.

2. Methods

This research uses a qualitative approach with case study methodology to understand in depth the collaborative strategies between the Indonesian National Police and various related institutions in improving digital literacy to prevent triangle scheme online fraud in the Makassar Police Headquarters jurisdiction. The qualitative approach was chosen because it allows exploration of meaning from participants' perspectives, while the case study method was chosen to examine phenomena in specific and contemporary contexts. This research

follows five case study elements according to Yin (2018): research question formulation, research propositions, units of analysis, logic linking data with propositions, and criteria for interpreting findings. Data sources used consist of primary and secondary data. Primary data was obtained through in-depth interviews with police officials, representatives of government and non-government institutions, academics, practitioners, and community members who are victims of online fraud. Secondary data was collected from policy documents, official institutional reports, scientific journals, and media news. Data collection techniques were conducted through semi-structured interviews, non-participatory observation, and documentation, with the aim of obtaining comprehensive information regarding the implementation and effectiveness of digital literacy strategies in facing cybercrime in the region.

3. Results and Discussion

3.1. Evaluation of the effectiveness of steps taken to improve digital literacy among the public in the Makassar Police Headquarters jurisdiction

Digital literacy becomes a main component in anticipating various cyber threats such as hoaxes and digital radicalism that are increasingly rampant. The strategy implemented by Makassar Police Headquarters (Polrestabes) shows that the success of digital literacy programs greatly depends on strong institutions, collaboration between internal functions, and the use of data as a basis for planning and evaluation (Tsaniyah & Juliana, 2019).

Digital literacy provides the ability for society to evaluate information critically and reduce the risk of being trapped in misleading content. This is important so that society does not easily become victims of fraud or the spread of negative content in cyberspace. Makassar Police Headquarters utilizes various communication channels and prioritizes active preventive approaches through socialization involving functional units (satfung) such as Community Guidance (Binmas) in direct education to the community, so this strategy does not only stop at information dissemination but also builds stronger social infrastructure (Fitriani, 2020).

The role of police institutions is also shown through programs targeting educational institutions and local communities as digital education centers, expanding the reach and impact of digital literacy programs. Collaboration with various external parties such as the Ministry of Communication and Informatics (Kominfo), Financial Services Authority (OJK), and digital communities becomes a key factor so that literacy efforts can run more effectively and comprehensively. Additionally, the utilization of data analysis to identify patterns of digital crime and hoax distribution enables Makassar Police Headquarters to conduct more focused and targeted interventions (Tropina, 2017).

Special training for police personnel also becomes an important part of these efforts so that officers are ready and capable of tackling digital challenges professionally. Nevertheless, challenges still arise regarding gaps in community access to digital technology, which can hinder achieving digital literacy evenly. Therefore, strengthening digital infrastructure and providing broader access becomes part of long-term strategies that need to be continuously developed to ensure digital security in society inclusively (Fitriani, 2020).

The institutional strategy implemented by Makassar Police Headquarters in improving community digital literacy can be classified into three main levels: policy, strategy, and operational efforts, each having clear legal foundations and implementation directions. At the policy level, Makassar Police Headquarters refers to the legal framework that serves as an

umbrella for implementing digital literacy programs, including Law Number 19 of 2016 concerning Information and Electronic Transactions (ITE Law) which regulates procedures for using information technology and electronic transactions while providing legal foundations for handling cybercrime. Additionally, the Indonesian National Police's (Polri) digital transformation policy through the Precision program launched by the Chief of Police strengthens the direction of police institutional modernization in the digital era, including the implementation of territorial unit duties according to Police Regulation Number 6 of 2019 concerning the Organization and Working Procedures of the Indonesian National Police (Polri) which regulates organizational structure and division of functional unit duties such as Community Guidance Unit (Satbinmas) and Intelligence Unit (Satintel).

At the strategy level, Makassar Police Headquarters conducts structured planning with clear time frame divisions: short-term through direct socialization and counseling to the community, medium-term with mapping of areas prone to digital crime to focus prevention efforts, and long-term through forming digital communities and strengthening sustainable social infrastructure. This strategy aligns with adaptive and data-based institutional strategy principles recommended in strategic management literature and Polri transformation directions that prioritize digitalization and multi-stakeholder collaboration (Police Regulation No. 6 of 2019).

At the operational level, implementation of operational programs shows optimal utilization of Makassar Police Headquarters's internal functions and resources in parallel and systematic ways. Community Guidance Unit (Satbinmas) is responsible for education and digital literacy socialization to the wider community, particularly vulnerable groups and active internet users. Traffic Unit (Satlantas) and Intelligence conduct data collection on mobile phone stores and public internet access points as part of risk mapping and strategic databases in preventing digital crime. Additionally, the Public Relations Division and Special Criminal Investigation Unit (Reskrimsus) produce and distribute digital educational content as effective communication media. These operational efforts are concrete implementations of policies and strategies regulated within Polri's legal framework, while reflecting institutional commitment to building inclusive and sustainable digital literacy systems.

Table 1. SWOT Analysis of Makassar Police Headquarters Digital Literacy Strategy Evaluation

Aspect	Internal Factors	External Factors
Strengths	1. Solid and organized Polrestabes institutional structure 2. National and local regulatory support 3. Availability of internal technical functions (Satbinmas, Satintel, Satlantas, Reskrimsus) 4. Direct access to community through routine activities	1. Government support in national digital transformation 2. Public trust in police digital literacy programs
Weaknesses	1. Uneven HR capacity in digital technology mastery 2. Suboptimal collaboration between functional units 3. Minimal special budget for digital literacy 4. Program distribution has not reached all peripheral areas	1. Low digital literacy among parts of society 2. Lack of digital infrastructure in remote areas
Opportunities	1. Potential collaboration with Kominfo, Komdigi, OJK, and educational institutions	1. Development of national regulations regarding digital crime

Aspect	Internal Factors	External Factors
	2. Access to social media and technology as educational tools 3. Support from digital communities and literacy volunteers	2. International institutional support for digital literacy programs
Threats	1. Slow institutional adaptation to technology 2. Potential work overload for technical functions without specialization 3. Increasingly complex spread of hoaxes and digital crime	1. Speed of digital technology evolution and online fraud methods 2. Threat to public trust if programs are inconsistent

The SWOT analysis of Makassar Police Headquarters in the context of community digital literacy improvement strategies shows a fairly comprehensive picture when related to the theories used and police institutional context. From the strengths side, Metropolitan Police's (Polrestabes) solid and organized institutional structure becomes the main foundation in running digital literacy programs. This aligns with Talcott Parsons' Social System Theory which places police as part of a social system that must be structured to function adaptively and maintain social order. The availability of internal technical functions such as Community Guidance (Satbinmas), Intelligence (Satintel), Traffic (Satlantas), and Special Criminal Investigation (Reskrimsus) provides a clear framework for coordinated task implementation, while strengthening operational bases in directly reaching the community. National and local regulatory support, including the ITE Law and Polri's Precision digital transformation policy, becomes a legal umbrella that affirms legitimacy and implementation direction of programs, while public trust in digital literacy programs opens opportunities for greater success through active community participation.

However, on the weaknesses side, there are still several obstacles that hinder program effectiveness. Uneven human resource (HR) capacity in digital technology mastery becomes a significant constraint that must be immediately addressed so that literacy programs are not merely formalities but truly impactful. This relates to the need for intensive training and competency development which is part of the Digital Literacy Implementation Model at the applied theory level. Additionally, suboptimal collaboration between internal functional units reflects a lack of synergy that could cause task overlap and inefficiency in program implementation. Limited special budgets for digital literacy also become real constraints, especially when compared to the complexity of continuously evolving threats. Program distribution that has not reached all peripheral areas indicates access gaps and uneven digital infrastructure development which becomes a real challenge, especially in geographically difficult-to-reach areas.

Looking at opportunities, Makassar Police Headquarters has considerable space to expand and deepen its digital literacy programs through collaboration with various external institutions such as Ministry of Communication and Informatics (Kominfo), Digital Communication Ministry (Komdigi), Financial Services Authority (OJK), and educational institutions. This opportunity is very important from the Community Policing Theory perspective which emphasizes active partnerships between police and community. Utilization of social media and technology as educational tools can also accelerate the spread of correct information and reduce misinformation risks. Support from digital communities and literacy volunteers represents potential resources that can strengthen program reach and impact. On the regulatory side, development of increasingly strict national regulations regarding digital crime and international institutional support provide strong foundations for effective law enforcement and prevention.

However, threats faced cannot be ignored. Slow institutional adaptation to digital technology development can make Metropolitan Police (Polrestabes) lag in responding to continuously evolving cybercrime modes. Risk of work overload on technical functions without specialization can reduce program effectiveness and focus, ultimately harming prevention processes. Increasingly complex spread of hoaxes and digital crime demands responses that are not only reactive but also proactive and sustainable. Threats to public trust if digital literacy programs are inconsistent or lack transparency can weaken police legitimacy and community participation. The speed of technology evolution and continuously changing online fraud methods also becomes a major challenge requiring continuous innovation.

At the Grand Theory level, namely Talcott Parsons' Social System Theory, Makassar Police Headquarters is viewed as an integral part of the social system that must be adaptive to maintain social order. Internal strengths such as solid and organized institutional structure and national and local regulatory support strengthen Metropolitan Police's (Polrestabes) position as an institution capable of performing its social functions in addressing digital challenges. The availability of internal technical functions such as Community Guidance (Satbinmas), Intelligence (Satintel), Traffic (Satlantas), and Special Criminal Investigation (Reskrimsus) provides structural foundations that enable organized and adaptive responses to community dynamics, consistent with harmonious and interconnected social system principles.

Moving to Mid-Range Theory, Community Policing Theory emphasizes the importance of active partnerships between police and community in preventing crime, particularly technology-based crime. From the opportunities side, collaboration potential with external institutions such as Ministry of Communication and Informatics (Kominfo), Digital Communication Ministry (Komdigi), Financial Services Authority (OJK), and educational institutions shows how Makassar Police Headquarters can expand partnership networks and increase digital literacy socialization effectiveness. Use of social media as educational tools and involvement of digital communities and literacy volunteers represents concrete implementation of this theory in practice. However, weaknesses such as suboptimal collaboration between internal functional units and uneven program distribution show remaining obstacles in building synergistic partnerships, which if addressed will strengthen effective community policing foundations.

At the Applied Theory level, the Digital Literacy Implementation Model helps explain how Makassar Police Headquarters implements operational steps in micro and practical ways. Uneven human resources (HR) capacity in digital technology mastery is a challenge that must be immediately addressed through intensive training and competency development. This is very important so that educational and socialization program implementation runs optimally and sustainably. Threats including hoax spread, increasingly complex digital crime, and potential work overload on technical functions demand specialization strategies and more sophisticated technology utilization for monitoring and prevention, which are part of operational efforts at the applied theory level. Consistency and innovation in these programs will determine Makassar Police Headquarters's success in building a resilient digital literacy ecosystem.

Integration of these three theories also shows how Makassar Police Headquarters must undergo transformation not only from structural and policy sides (grand theory) but also from partnership relationships with community and other institutions (mid-range theory), to technical implementation of programs oriented toward concrete results (applied theory). By optimizing strengths and opportunities through this framework, Metropolitan Police (Polrestabes) can overcome internal weaknesses and mitigate external threats systemically

and sustainably. This approach enables digital literacy programs to become not only formal tasks but integral parts of national cyber security strategies capable of educating society and strengthening public trust in police.

The institutional strategy model of Makassar Police Headquarters in improving community digital literacy reflects implementation of systematic and tiered approaches, starting from macro policies to micro program implementation. At the policy level, Makassar Police Headquarters is based on national regulations such as the Information and Electronic Transaction Law (ITE Law), Police Regulation No. 23 of 2010 concerning Organizational Structure and Working Procedures, and Indonesian National Police's (Polri) Precision digital transformation policy from Police Headquarters. These legal foundations and policies become umbrellas that direct and integrate all digital literacy programs to align with national standards and current information technology developments.

Furthermore, at the strategy level, Makassar Police Headquarters divides planning in detail based on time frames, including short, medium, and long term. In the short term, focus is directed toward socialization and education through social media and Community Guidance (Binmas) activities that directly touch the community. Medium term emphasizes mapping areas prone to digital crime by involving intelligence functions, so prevention efforts can be more targeted and responsive to cyber threat dynamics. For long term, Metropolitan Police (Polrestabes) develops digital social infrastructure in the form of digital law-aware communities and cybercrime early warning systems, which are expected to build sustainable digital security ecosystems in their jurisdiction.

At the operational or micro level, concrete steps implemented involve various internal technical functions of Makassar Police Headquarters. Community Guidance Unit (Sat Binmas) actively conducts socialization and education in schools, campuses, and communities to strengthen community digital literacy. Traffic Unit (Satlantas) and Intelligence Unit (Intelkam) play roles in data collection of mobile phone stores and public WiFi networks as part of mapping potential digital misuse. Additionally, formation of specialized digital information teams involving Public Relations and Special Criminal Investigation (Reskrimsus) functions enables effective production and distribution of educational content. This model illustrates integrated and complementary institutional strategies from policy to implementation, enabling Makassar Police Headquarters to respond to digital literacy challenges with adaptive, collaborative, and data-based approaches.

3.2. Strategic Policy Recommendations for Improving Digital Literacy as an Effort to Prevent Online Fraud Using Triangle Scheme Methods More Effectively and Sustainably

The Fraud Triangle scheme, consisting of three main components—pressure, opportunity, and rationalization provides a strong theoretical framework for explaining the dynamics and motivations behind fraudulent acts, including in the context of online fraud such as romance scams. These three elements not only work individually but also mutually reinforce each other and create conditions that enable fraud to occur.

First, pressure refers to the internal conditions of perpetrators that create a strong drive to commit fraud. In the context of online fraud, this pressure often stems from urgent economic needs, such as poverty, debt, unemployment, or the desire to maintain a certain lifestyle that is not proportional to available resources. Barnor et al. (2020) argue that this pressure becomes the main triggering factor that drives individuals to seek illegal shortcuts through digital-based fraud schemes. In many cases, perpetrators experience failure in achieving financial goals through legitimate means, so psychological pressure to survive triggers deviant behavior.

Second, opportunity refers to the availability of means or situations that allow perpetrators to carry out their actions without high risk of being caught. In the digital era, the internet has created enormous opportunities for perpetrators to target victims from various backgrounds and geographical locations. Anonymity, ease of creating fake identities, and weak identity verification systems on social media platforms and dating applications have increased the chances of fraud success. Barnor et al. (2020) note that widespread access to information technology allows perpetrators to conduct systematic and repeated attacks with minimal costs and low legal risks, especially when conducted across countries.

Third, rationalization is a cognitive process where perpetrators justify their fraudulent actions as something legitimate or acceptable. In romance fraud, perpetrators often build narratives that victims are parties who are "capable" or "naive," so money taken is not considered a form of cruel exploitation. Rationalization also often appears in the form of assumptions that social or economic systems have failed to provide justice, so fraudulent actions are viewed as a form of "revenge" or fair compensation (Barnor et al., 2020). In other words, rationalization functions to eliminate guilt and maintain the perpetrator's self-image as an individual who remains "moral."

However, although the Fraud Triangle structurally explains how fraud can occur, it is important to note that not all individuals who experience pressure or have opportunities will choose the path of fraud. Protective factors such as personal moral values, ethics education, social environment, and strict supervision or law enforcement can be significant barriers. In this case, the Fraud Triangle needs to be contextualized with moral psychology perspectives and social control theory that explain why some people still choose honest behavior despite being under pressure and having opportunities to deviate.

Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE Law) is the main legal umbrella regulating digital activities in Indonesia, including regulating online fraud crimes. Article 28 paragraphs (1) and (2) of the ITE Law explicitly prohibit the dissemination of misleading information and fraud through electronic systems. However, although this law has provided a legal basis for prosecuting perpetrators of triangle scheme fraud, its implementation still faces significant challenges, such as low public awareness of their rights and obligations in the digital realm and lack of adequate digital literacy. This shows that education and digital literacy aspects need to be strengthened so that the public not only understands legal prohibitions but is also able to recognize and prevent fraud independently.

In addition, the Criminal Code can also be used to prosecute fraud perpetrators with articles on fraud (Article 378 of the Criminal Code), but the success of enforcement still depends on the capacity of law enforcement officers to understand and handle cases involving digital technology. Therefore, strengthening the capacity of law enforcement human resources and establishing special cybercrime handling units becomes a strategic need so that the implementation of the ITE Law and Criminal Code can run effectively.

On the other hand, the Consumer Protection Law (Law No. 8 of 1999) and the Personal Data Protection Law (Law No. 27 of 2022) open opportunities to expand the legal framework for preventing online fraud. Digital literacy must include understanding of digital consumer rights and personal data protection, so that the public is not easily trapped in fraud schemes that illegally exploit their personal data.

The strategy for improving digital literacy as an effort to prevent online fraud, especially triangle scheme methods, requires a comprehensive and sustainable approach. Analysis shows that the effectiveness of these measures is greatly influenced by institutional aspects, human resource capacity, and collaboration between stakeholders. One of the main challenges is the gap in mastering digital technology among police officers and the community, as well as the

suboptimal synergy between functional units in implementing digital literacy programs. In addition, budget limitations and uneven program distribution, especially in peripheral areas, are also significant obstacles. On the other hand, opportunities in the form of strong national regulatory support, advances in communication technology, and potential collaboration with various external institutions open strategic space for developing more effective programs. However, threats in the form of rapid development of digital crime methods and the spread of hoax information require Makassar Police Headquarters to be more adaptive and innovative in prevention strategies.

In efforts to improve digital literacy as a strategy for preventing online fraud with triangle scheme methods, strengthening regulation and law enforcement is a very crucial step. Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE Law) must be strengthened with the establishment of clear and effective sanctions to provide a deterrent effect for fraud perpetrators (Wang et al., 2020). The formation of special task forces focused on handling online fraud is needed to accelerate the law enforcement process transparently and responsively, in line with the principle of efficiency in the criminal justice system (Tyler, 2006). Easy and fast reporting mechanisms for victims are also essential so that criminal acts can be immediately followed up.

Digital education and literacy need to be systematically integrated into formal education curricula from elementary to university levels. Effective digital literacy will provide the ability for the public to recognize various online fraud methods and increase vigilance (Livingstone et al., 2011). Educational modules and digital literacy training that are easily accessible to the general public, both online and offline, are empowerment strategies consistent with community empowerment theory (Zimmerman, 2000), which emphasizes increasing individual and community capacity in facing social challenges.

The concept of Community Policing is very relevant in the context of preventing digital crimes, including online fraud. Community Policing emphasizes partnerships between police officers and the community to increase community participation in maintaining security (Skogan, 2003). Therefore, ongoing and integrated socialization campaigns involving community leaders, digital influencers, and the private sector through various media are effective for building public awareness and vigilance against online fraud.

Cross-sector collaboration is an important aspect in combating online fraud. According to Ansell & Gash (2008), collaborative governance theory emphasizes the importance of cooperation between various stakeholders in solving complex public problems, including cybercrime. The formation of communication and coordination forums between institutions can strengthen information exchange and integrated countermeasure strategies.

In addition, the development of supporting digital technology and infrastructure, such as fraud early detection systems and real-time transaction verification applications, should be pursued to help the public conduct independent checks and avoid fraud risks (Kodmalwar et al., 2024). Providing equitable and affordable internet access is also a prerequisite so that digital literacy programs can be accessed by all levels of society, supporting digital inclusivity.

Finally, regular monitoring and evaluation of digital literacy programs and law enforcement is essential to ensure policies remain relevant and effective in facing the dynamics of fraud methods and technological advances (Patton, 2008). All these efforts must be in line with applicable legal frameworks, especially the ITE Law, Consumer Protection Law, and Personal Data Protection Law, and prioritize transparency and accountability in handling online fraud cases (Kshetri, 2013). Adoption of international best practices is also recommended so that policies can be adaptive and sustainable.

In efforts to improve digital literacy as a preventive step against online fraud with triangle scheme methods, comprehensive strengthening of regulation and law enforcement needs to be carried out. Regulations related to cybercrime, especially those contained in Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE Law), must be revised and strengthened to contain clearer sanctions and provide deterrent effects. The formation of special task forces that focus on handling online fraud cases is very important to accelerate the law enforcement process transparently and responsively. In addition, developing reporting mechanisms that are easily accessible to victims is a strategic need to support more effective legal processes.

In terms of education, integration of digital literacy programs that include understanding of online fraud methods needs to be systematically implemented in formal education curricula from elementary school to university levels. Development of educational modules and digital literacy training that can be widely accessed by the general public, both through online and offline platforms, is an important instrument in increasing community capacity in facing digital crime risks. Empowering digital libraries, community groups, and non-governmental organizations as education centers is also a strategic step to expand digital literacy coverage.

In addition, ongoing and integrated socialization campaigns through various mass media, including social media, television, radio, and print media, are essential to increase public awareness of the dangers of online fraud using triangle scheme methods. Involving community leaders, digital influencers, and the private sector in delivering socialization messages will expand the reach and effectiveness of these campaigns with simple language approaches and attractive visualizations.

Cross-sector collaboration between government, law enforcement agencies, private sector especially digital platforms and fintech, academics, and civil society must be enhanced. The formation of cross-sectoral coordination and communication forums enables information exchange and more comprehensive and integrated prevention strategy synergy.

Digital technology and infrastructure development is also an equally important aspect. Improving filter systems and early detection on digital platforms to anticipate triangle scheme fraud methods, as well as developing applications or real-time transaction verification systems, need to be pursued to improve community ability to identify and avoid fraud risks. Providing equitable and affordable internet access is a main prerequisite so that digital literacy programs can be effectively reached by all levels of society.

Implementation of digital literacy programs and law enforcement must be followed by systematic and continuous monitoring and evaluation mechanisms to ensure policy effectiveness and relevance according to the dynamics of technological development and fraud methods. All these policies need to be developed within a strong legal framework, taking into account the Electronic Information and Transactions Law (ITE Law), Consumer Protection Law, and Personal Data Protection Law. Strengthening aspects of transparency, accountability, and adoption of international standards in handling cybercrime will make these policies adaptive and sustainable in facing challenges in the digital era.

4. Conclusion

This research concludes that the strategy for preventing online fraud with triangle scheme methods in the jurisdiction of Makassar Police Headquarters has not been implemented optimally, despite existing institutional frameworks, regulations, and internal resources that support it. Digital literacy improvement efforts carried out by Makassar Police Headquarters through institutional and collaborative approaches still face various structural and operational obstacles, including: capacity gaps in human resources in mastering digital technology, suboptimal synergy between internal functional units, and program distribution that has not evenly reached peripheral areas vulnerable to cybercrime.

Nevertheless, institutional strength and national regulatory support such as Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE Law), Law Number 27 of 2022 concerning Personal Data Protection, and Police digital transformation policies through the Precision program are important foundations in forming a directed digital literacy system. The digital literacy strategy implementation model developed by Makassar Police Headquarters has covered three main levels such as policy, strategy, and operational but needs to be strengthened through integration of comprehensive training systems, expansion of digital access, and increased community participation.

Theoretically, the integration between Social System Theory, Community Policing, and Digital Literacy Implementation Model in this research proves that the effectiveness of cybercrime prevention strategies is not only determined by legal and institutional structures, but also by success in building active partnerships with communities and the private sector. The concept of collaborative governance becomes important in addressing the complexity of digital crimes involving various cross-sector actors.

The role of Makassar Police Headquarters as the main actor in maintaining digital security at the local level needs to be directed not only at enforcement, but also at community empowerment as active subjects in digital space surveillance. Digital literacy improvement efforts cannot be sporadic, but must be developed continuously with support from equitable technology infrastructure and monitoring and evaluation systems that are adaptive to digital crime dynamics. Thus, digital literacy-based online fraud prevention strategies demand reformulation of policy approaches that are more integrated, innovative, and long-term oriented. This approach not only supports law enforcement effectiveness, but also strengthens police social legitimacy in the era of complex digital transformation.

5. References

Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, *18*(4), 543–571.

Barnor, J. N. B., Boateng, R., Kolog, E. A., & Afful-Dadzie, A. (2020). Rationalizing online romance fraud: In the eyes of the offender. *26th Americas Conference on Information Systems, AMCIS 2020*.

Fitriani, S. (2020). Perpustakaan Dan Gerakan Sadar Literasi Sebagai Upaya Menangkal Hoaks. *Jurnal Ilmu Perpustakaan Dan Informasi Islam*, *01*(01).

Guntik, D. S., & Yustiawan, D. G. P. (2022). Corporations As Whistleblowers In The Crime Of Defamation Based On The Electronic And Transaction Information Act. *Policy, Law, Notary and Regulatory Issues (POLRI)*, *1*(1), 65–73. https://doi.org/https://doi.org/10.55047/polri.v1i1.43

Januri, J., Melati, D. P., & Muhadi, M. (2022). Upaya Kepolisian Dalam Penanggulangan Kejahatan Cyber Terorganisir. *Audi Et AP : Jurnal Penelitian Hukum*, *1*(02). https://doi.org/10.24967/jaeap.v1i02.1692

Kasim, Z. (2024). Kebijakan Hukum Pidana untuk Penanggulangan Cyber Crime di Indonesia. *Indragiri Law Review*, *2*(1), 18–24. https://doi.org/10.32520/ilr.v2i1.22

Kodmalwar, P., Maheshwari, A., Palav, M., Priya, S., Purusothaman, N., & Namdeo, A. (2024). *Real-Time Fraud Detection Using AI and Signal Processing* (pp. 121–136). https://doi.org/10.4018/979-8-3693-7367-5.ch009

Kshetri, N. (2013). *Cybercrime and cybersecurity in the global south*. Springer.

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries*.

Patton, M. Q. (2008). *Utilization-focused evaluation*. Sage publications.

Rahman, Z. A. (2024). Pemanfaatan Teknologi Informasi dalam Edukasi Literasi Digital untuk Peningkatan Keamanan Data dan Pencegahan Kejahatan Siber di Masyarakat Rawang Panca Arga. *Merkurius : Jurnal Riset Sistem Informasi Dan Teknik Informatika*, *2*(6), 82–90. https://doi.org/10.61132/merkurius.v2i6.399

Rumata, V. M. (2017). Komunikasi Keluarga Masyarakat Kota Dan Desa Di Era Teknologi Komunikasi. *Journal Pekommas*, *2*(1). https://doi.org/10.30818/jpkm.2017.2020105

Skogan, W. G. (2003). *Community policing: Can it work?* Wadsworth Publishing Company.

Tropina, T. (2017). Cyber-policing: the role of the police in fighting cybercrime. *European Law Enforcement Research Bulletin*, *2*.

Tsaniyah, N., & Juliana, K. A. (2019). Literasi Digital Sebagai Upaya Menangkal Hoaks Di Era Disrupsi. *Al-Balagh : Jurnal Dakwah Dan Komunikasi*, *4*(1). https://doi.org/10.22515/balagh.v4i1.1555

Tyler, T. R. (2006). *Why people obey the law*. Princeton university press.

Wang, J., Li, S., & Guo, W. (2020). The role of legal frameworks in combating cybercrime: A comparative study. *Computer Law & Security Review*. https://doi.org/10.1016/j.clsr.2020.105381

Yin, R. K. (2018). *Case study research and applications* (Vol. 6). Sage Thousand Oaks, CA.

Zimmerman, M. (2000). Empowerment Theory: Psychological, Organizational and Community Levels of Analysis. *Handbook of Community Psychology*.