COMPENDIUM OF JUDGE MADE LAWJOURNAL
Volume 1 Issue 2 Year 2025

The Dilemma of Law Enforcement in Determining Suspects in Online Gambling Site Promotion Cases: A Case Study at the South Sulawesi Regional Police

Muhammad Agung Hidayah[1], La Ode Husen[2], Muhammad Azham Ilham[3]

[1]*Fakultas Hukum, Universitas Muslim Indonesia, Indonesia*
[2]*Fakultas Hukum, Universitas Muslim Indonesia, Indonesia*
[3]*Fakultas Hukum, Universitas Muslim Indonesia, Indonesia*

Email Correspondence: muhammadagunghidayah11@gmail.com

Abstract: This study aims to identify and analyze the obstacles faced by the police in determining suspects in cases involving the promotion of online gambling sites through information technology. This research employs an empirical legal research method, which examines the application of legal norms based on real conditions in the field. Data were collected through interviews, observations, and a literature review of primary and secondary legal materials. The study was conducted at the Regional Police of South Sulawesi (Polda Sulsel).The results indicate that the legal procedure for determining suspects in online gambling promotion cases at Polda Sulawesi Selatan involves several stages: investigation, inquiry, collection of valid evidence, and witness examination. Once at least two sufficient pieces of evidence are obtained in accordance with the Indonesian Criminal Procedure Code (KUHAP), the investigator formally determines the perpetrator as a suspect. Law enforcement is carried out carefully, as offenders often disguise their digital identities using fake accounts, virtual private networks (VPNs), and proxy servers. The main challenges faced by the police include difficulties in tracing perpetrators' identities due to digital obfuscation, limited access to encrypted communication data, and the lack of public participation in reporting online gambling promotion activities. These findings highlight the importance of improving investigators' technical capacity and strengthening inter-agency cooperation, particularly with the Ministry of Communication and Informatics and digital platform providers, to enhance the effectiveness of law enforcement against cybercrime based on information technology.

Keywords: suspect determination*;* online gambling*;* site promotion*;* law enforcement*;* information technology;

A. INTRODUCTION

Gambling has been around for a long time and remains quite popular today. Classifying gambling as a crime reflects its status as a collective disease. Due to the harm it can cause to the social fabric of society, gambling is illegal in many religions, including Islam, which also considers gambling and betting sinful or haram (forbidden).[1] Many types of online gambling are promoted through advertisements on websites, and their widespread distribution makes it extremely difficult to stop. One such social pathology is the marketing of gambling websites. Advertising gambling sites online encourages people to try gambling themselves, which poses a danger to social standards and, by extension, the social order. Consequently, the promotion of online gambling sites can hinder technical innovation, remove the human element, and hinder national growth in the material and spiritual realms.[2] Now, more than ever, people are

openly promoting online gambling companies using YouTube apps, rather than hiding behind anonymous websites. This is despite the fact that Article 303 of the Indonesian Criminal Code regulates gambling laws, and the Electronic Information and Transactions (ITE) Law regulates all forms of online gambling, including the support of online gambling, within the country. [3]

Any game in which the probability of winning depends largely on chance, even when the player may have superior training or talent, is considered a game of chance under Article 303 paragraph (3) of the Criminal Code.[4] Included in this category are all regulations, including those relating to determining the winner of a contest or game that does not involve direct interaction between players. In response to the widespread misuse of information technology for criminal purposes, particularly online gambling, the state enacted Article 27 paragraph (2) of the ITE Law. Gambling in Indonesia has shifted to the digital realm, becoming more covert and accessible to a larger demographic, particularly young people, as a result of the development of online and social media in the country.[5] Both the general public and policymakers are beginning to recognize that online gambling has far-reaching negative consequences, including economic loss, social instability, family disintegration, and mental health problems. Online gambling, especially when presented in subtle forms such as endorsements, affiliations, or promotions, poses serious ethical and legal challenges due to the ease with which users can access gambling platforms through social media, chat programs, and hidden websites.[6] There has been a dramatic increase in the number of cases of prominent and influential figures in Indonesia supporting or promoting online gambling in 2024. The spread of illicit information through social media platforms has made this issue a major concern for law enforcement and the general public. This example is quite significant.[7]

After promoting an online gambling site for almost a year and collecting Rp. 250,000 in regular installments, a counter developer with the initials MRA (19) was arrested. The Head of Sub-Directorate 5 of the Criminal Investigation Directorate of the South Sulawesi Regional Police, Commissioner Bayu Wicaksono Febrianto, S.Ik, stated that MRA only promoted himself on a social media site and had no direct involvement in online gambling activities. The Makassar District Court found MRA (19) legally and convincingly guilty of violating Article 45 (2) and Article 27 (3) of Law Number 1 of 2024, which is the second amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE). The court sentenced MRA to 20 months in prison. Due to its negative impacts on ethics, religion, and society, gambling is strictly prohibited in Islam. From the perspective of Islamic law, gambling is strictly prohibited because it contradicts the principles of honesty, justice, and the attainment of lawful and blessed sustenance. Islam teaches that wealth must be acquired through lawful means, hard work, and legitimate effort. This is as affirmed in the word of Allah SWT: “O you who believe! Indeed, intoxicants, gambling, [sacrificing on] stone altars, and divining arrows are but defilement from the work of Satan, so avoid them that you may be successful.” (QS. Al-Ma’idah: 90). This verse emphasizes that gambling is a prohibited act as it contains elements of falsehood, undermines moral values, and has the potential to cause widespread social harm. Therefore, the phenomenon of promoting online gambling sites is not merely a violation of positive law, but also a threat to moral values, social ethics, and societal stability. Accordingly, an empirical study is necessary to analyze the obstacles faced by law enforcement authorities,

particularly the police, in determining suspects in cases involving the promotion of online gambling through information technology. This research is expected to contribute to strengthening cyber law enforcement policies that are more effective, adaptive, and responsive to the dynamics of digital crime in Indonesia.

B. METHOD

This research method is empirical legal research, Empirical Legal Research Method is a legal research method that uses empirical facts taken from human behavior, both verbal behavior obtained from interviews and real behavior carried out through direct observation.[8] The location of this research was carried out at the South Sulawesi Provincial Police Office (POLDA Sulsel), this research location was chosen because it is representative for the author's research. This research uses the following types and sources of data: primary data, data obtained directly from the source either through interviews, observations and unofficial document reports which are then reprocessed by the researcher; secondary data such as obtained by conducting library research on the research materials used which include, literature books, journals, legislation, legal articles, scientific papers, written documents/archives, data, and readings. The data obtained through research activities are analyzed qualitatively and then presented descriptively, namely by describing, explaining, and describing according to the problems relevant to this research.

C. DISCUSSION

1. Legal Procedures for Determining Suspects in Site Promotion Cases in Online Gambling Cases

The problem of online gambling is increasingly disturbing the public, as evidenced by the increasing number of illegal online gambling sites, the use of social media and instant messaging apps for promotion, and the increasing number of perpetrators and victims, including teenagers and young adults. [9] This clearly visible activity can undoubtedly create problems that are sometimes difficult to stop because online soccer and poker gambling utilize information technology. This represents a form of criminal development and the use of electronic transactions. The number of online gambling cases in South Sulawesi between 2021 and 2024 continues to increase, as clearly seen in the following table:

No.	Tahun	CT	CC	SIDIK	P21/TAHAP ll
1	2021	-	-	-	-
2	2022	1	1	-	1
3	2023	5	3	2	3
4	2024	7	6	1	6
	Jumlah				

Description:
1.CT = Total Crime (Number of Cases)
2.CC = Crime Clearance (Cases Completed)

A recapitulation of data on online gambling crimes handled by Sub-Directorate V of the Special Criminal Investigation Directorate of the South Sulawesi Regional Police shows a significant increase in the number of reported and prosecuted cases from 2021 to 2024. Based on available data, there were no reports or cases related to online gambling in 2021. This could be interpreted as a sign that online gambling had not yet become a priority issue, or possibly a low level of reporting from the public or findings by law enforcement officials during that year.

Entering 2022, there was an increase, with one case report (CT) being immediately followed up and successfully transferred to prosecution (P21/Stage II). This marks the beginning of an active response by law enforcement officials to the growing number of information technology-based crimes.

The upward trend continued in 2023, with the number of reports increasing to five, with three cases successfully solved and two still under investigation. Three of these cases have been resolved and handed over to the prosecutor's office. This data indicates an intensification of law enforcement against cybercrime, particularly related to the increasingly widespread practice of online gambling.

According to Police Brigadier Muhammad Aksan, online gambling represents an improvement or upgrade on previous forms of gambling. Online gambling is a game of chance that uses a computer or mobile phone that can be accessed via Wi-Fi or a cellular internet network. Online gambling itself is actually regulated in the law that regulates online gambling in Indonesia, namely Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which has been amended by Law Number 1 of 2024. Specifically, Article 27 paragraph (2) of the ITE Law regulates the prohibition of online gambling, which reads: "Any person who intentionally and without the right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents containing gambling content." And Article 45 regulates the sanctions, which reads: "Any person who fulfills the elements as referred to in Article 27 paragraph (2) shall be punished with imprisonment for a maximum of 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiah).

In determining the suspect for online gambling promotion on social media, the South Sulawesi Regional Police's Cyber Crime Unit has several stages, namely:[10]

1. Preliminary Investigation

   According to Article 1 (1) number 5 (5) of the Criminal Procedure Code, an investigation is a series of investigative actions to locate and discover an event suspected of being a crime in order to determine whether an investigation can be conducted according to the procedures stipulated in the law. Investigations into online gambling crimes, particularly those conducted through promotional practices on social media and digital platforms, are one of the primary duties of the police cybercrime unit. In this context, investigators actively observe and track suspicious activity, both on platforms such as Instagram, websites, and video-based channels like YouTube. Endorsement or promotion of online

gambling content is often disguised as entertainment, app reviews, or indirect links, requiring in-depth and ongoing monitoring.

As a first step, investigators utilize digital forensics technology and specialized tools such as open-source intelligence tools (OSINT), network traffic analyzers, and digital footprint trackers to identify perpetrators, observe content distribution patterns, and trace the connections between involved accounts. The use of this technology aims to collect legally valid digital evidence, such as metadata, IP addresses, activity logs, and the contents of electronic communications that indicate intent and involvement in gambling activities. According to Brigadier Muhammad Aksan, handling online gambling promotion cases presents its own set of difficulties. One of the main challenges is the potential for the alleged perpetrator to flee if they become aware of the investigation. Therefore, the strategy employed by investigators in the initial stages is to conduct discreet, remote observation to avoid suspicion. Next, investigators will attempt to collect at least two pieces of valid and relevant evidence as a requirement to elevate the suspect's status to suspect during the investigation.

2. Collection of Evidence

Evidence collection is a fundamental stage in the criminal investigation process, including in cases of online gambling promotion. This stage aims to obtain a strong legal basis in determining someone as a suspect and proving the elements of the alleged crime. Based on the provisions of Article 184 of the Criminal Procedure Code (KUHAP), valid evidence consists of witness statements, expert statements, letters, clues, and statements from the suspect. In practice, determining someone as a suspect must be based on at least two valid pieces of evidence and accompanied by the investigator's belief that a crime has occurred. In the context of crimes committed through electronic media such as online gambling promotion, the characteristics of evidence have expanded due to the involvement of information and communication technology elements. According to Brigadier Gihon Life Purba, electronic evidence plays a very important role in revealing the modus operandi, communication patterns, and flow of financial transactions related to online gambling activities. This is in line with the provisions of Article 5 paragraph (1) of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which states that electronic information and/or electronic documents and their printouts constitute valid legal evidence.

Forms of electronic evidence in online gambling promotion cases may include, among other things: [11]

1. Promotional video or audio recordings uploaded to social media or digital platforms, demonstrating the perpetrator's efforts to attract public participation in gambling.
2. Screenshots of web pages, social media accounts, or instant messaging applications containing promotional content, links to gambling sites, or invitations to participate in online betting activities.
3. Records of electronic financial transactions, such as fund transfers from or to accounts identified as belonging to bookmakers or online gambling site

operators. This evidence is often used to trace the flow of funds and identify profiteers.

4. Digital log data, including server metadata, IP addresses, and website access history that demonstrate the suspect's activities in creating, distributing, or managing gambling promotional content.
5. Electronic correspondence, such as WhatsApp messages, Telegram messages, or emails containing communications between promoters and online gambling organizers.

The existence of this electronic evidence is highly significant because it can demonstrate the element of intent (mens rea) on the part of the perpetrator in distributing gambling content through electronic media. This element of intent is a crucial element in proving the case, as the perpetrator must be known to have had the intent and full awareness of their actions, which violate the law. Furthermore, in investigative practice, investigators can also use the testimony of digital forensic experts to ensure the authenticity and integrity of electronic evidence. Digital forensic experts play a role in verifying metadata, tracing file sources, and ensuring that the evidence has not been manipulated. This is crucial to ensure that evidence presented in court is admissible and has strong evidentiary value in accordance with the principle of chain of custody, namely the unbroken chain of control of evidence from the initial seizure to its presentation in court.

3. Case Title

The initial stage in the criminal law enforcement process begins with an inquiry and investigation, two crucial phases in uncovering a criminal incident. This stage primarily aims to determine whether an incident truly contains elements of a crime and who can be held legally accountable for it. An investigation is a series of initial actions taken by law enforcement officials to locate and identify events suspected of being criminal. The legal basis for this is regulated in Article 1, number 5 of the Criminal Procedure Code (KUHAP), which states that an investigation is "a series of actions by investigators to locate and identify an event suspected of being a crime in order to determine whether or not an investigation can be conducted according to the methods stipulated in law." Therefore, at this stage, police officers focus on fact-finding and initial identification of an incident, without determining a suspect.

If the results of the investigation indicate that the incident contains elements of a crime, the next stage is an investigation. According to Article 1, number 2 of the KUHAP, an investigation is a series of actions by investigators, in matters and according to methods stipulated in law, to seek and collect evidence, which can shed light on the crime that occurred and identify the suspect. The investigation phase is a more formal and in-depth phase than a preliminary inquiry because it focuses on establishing evidence and identifying the perpetrator. In practice, the process of gathering sufficient preliminary evidence is the core of investigative activities. Preliminary evidence serves as the legal basis for elevating a case from pre-investigation to investigation. Based on Article 184 of the Criminal Procedure Code (KUHAP), valid evidence consists of: witness testimony, expert testimony, letters, clues, and suspect testimony.

Furthermore, developments in national law, through Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), as amended by Law Number 19 of 2016, have expanded the scope of evidence to include electronic information and/or electronic documents as valid evidence (Article 5 paragraph (1) of the ITE Law). This demonstrates the legal system's adaptation to the dynamics of modern crime, including cybercrimes such as online gambling promotions, online fraud, and digital-based financial crimes. The investigator plays a central role in the investigation process. Investigators are responsible for gathering all relevant evidence to clearly describe the modus operandi of the crime, the motive, and the relationship between the perpetrator and the crime. Investigators' duties also include verifying and validating evidence, examining witnesses, requesting expert testimony, and preparing an investigation report (BAP), which will serve as the basis for subsequent prosecution.

This process must be conducted professionally, systematically, and accountably to ensure that the evidence obtained meets legal evidentiary standards and can be admissible in court. The principle of due process of law requires investigators to act in accordance with legal procedures, safeguarding the rights of suspects and witnesses, and ensuring the integrity of evidence through the chain of custody system, which ensures unbroken control of evidence from the initial seizure to its presentation in court.

4. Investigation

According to Mokhamad Najih, an investigation is "a series of actions carried out by investigators in accordance with the procedures stipulated by law to seek and collect evidence that sheds light on the criminal act and identify the suspect."

In the process of investigating online gambling promotion crimes, police officers, particularly investigators in the Cyber Unit, conduct location tracking to determine the perpetrator's whereabouts. Once the perpetrator's location is identified, investigators can immediately take repressive action in the form of an arrest without first issuing a summons or notification. However, such an arrest must still be based on an official warrant in accordance with applicable law.

Once the perpetrator is apprehended, investigators will proceed with a search of the premises suspected of storing equipment or evidence used in online gambling promotion activities. Furthermore, the evidence found will be confiscated for use in legal proceedings. Investigators may also detain the suspect to ensure the smooth running of the investigation and prevent the possibility of escape or destruction of evidence. After the suspect has been secured along with the confiscated evidence, investigators will continue the process by examining the suspect, witnesses, and expert witnesses appointed by the investigators. This examination is part of an effort to complete the elements of evidence needed before the case file is handed over to the prosecutor's office. In this stage, investigators refer to the provisions of Article 184 of the Criminal Procedure Code (KUHAP), which states that valid evidence

includes witness testimony, expert testimony, and testimony from the defendant himself.

5. Digital Forensic Testing

Digital forensics is a crucial stage in the process of proving criminal acts involving information technology. Generally, digital forensics can be defined as the process of identifying, collecting, analyzing, and interpreting electronic evidence with the aim of scientifically uncovering legal facts. According to international standards used by law enforcement agencies in various countries, digital forensics ensures that collected digital data can be authenticated and meets the formal and material requirements for admissibility as evidence in court.

The primary goal of digital forensics is to recover, secure, and analyze electronic data that may have been deleted, damaged, or modified. This process is crucial because digital criminals often attempt to erase traces of their activities using encryption techniques, permanent data deletion, or metadata manipulation. Through digital forensic methods, investigators can recover hidden data, trace network activity, and trace the source of communications or transactions related to crimes such as online gambling promotions, cyber fraud, and other electronic financial crimes.

In practice, digital forensics is divided into four main branches: [12]

1. Computer Forensics

This branch focuses on examining computers, laptops, and digital storage media, such as hard disks, flash drives, or solid-state drives (SSDs). The primary goal is to identify files, documents, system activity logs, and other digital traces that indicate user involvement in criminal activity. In the case of online gambling promotions, for example, computer forensic analysis can uncover data in the form of gambling site scripts, money transfer records, or promotional files distributed via the internet.

2. Mobile Device Forensics

This branch deals with the analysis of data contained on mobile devices such as smartphones, tablets, and other handheld communication devices. Through mobile forensics, investigators can obtain evidence in the form of text messages, call recordings, social media applications, GPS locations, and even digital transaction histories. This forensics is highly relevant in modern cases because most illegal communication and promotional activities are now conducted through applications such as WhatsApp, Telegram, or Instagram.

3. Network Forensics

Network forensics focuses on monitoring and analyzing data traffic on computer networks or the internet to identify communication patterns or suspicious activity. This process involves tracking IP addresses, analyzing data packets, and monitoring server logs to identify the origin and destination of data. In the context of online crime, network forensics can reveal how perpetrators access gambling

sites, the servers used to distribute content, or the relationships between multiple devices within the same criminal network.

4. Database Forensics
   This branch focuses on the analysis of database systems that store critical information, such as financial transaction records, customer data, or server configurations. Database forensics aims to identify unauthorized modifications, data theft, or attempts to conceal illegal transactions. In the case of online gambling, this technique can be used to audit transaction records between users and operators of online gambling sites.

In addition to these four branches, the digital forensics examination process must adhere to the principles of evidentiary law to ensure the results have legal validity in court. The primary principle that must be maintained is data integrity, meaning electronic evidence must remain unaltered from the moment it is discovered until it is presented in court. Therefore, every action taken on digital evidence must be documented in detail in the chain of custody to ensure its authenticity and uncontaminated nature.

In Indonesian law enforcement, digital forensic findings are often used to strengthen other evidence, as stipulated in Article 184 of the Criminal Procedure Code and Article 5 of the Electronic Information and Transactions Law. Findings from digital forensics can serve as legal clues (circumstantial evidence) that demonstrate the connection between the perpetrator and the criminal act. Therefore, digital forensic testing is not merely technical but also an integral part of the legal evidence process, ensuring certainty, justice, and accountability in resolving IT-based criminal cases.

Although all four have similar primary functions, namely recovering data, both in its original form and after deletion, each has a distinct focus.

Computer forensics focuses more on computer systems and the analysis of electronic documents. Meanwhile, mobile device forensics focuses on systems running on mobile digital devices such as smartphones.[13] Network forensics monitors and analyzes internet network activity, including data collection and detecting hacking or intrusion attempts. Database forensics focuses on examining the structure and content of databases, such as files, activity logs, and data in RAM, for the purposes of recovering and analyzing sensitive or strategic digital data.

The author believes that the arrest procedures carried out by the South Sulawesi Regional Police Cyber Unit in handling the online gambling promotion case followed applicable criminal procedural law, specifically as stipulated in the Criminal Procedure Code (KUHAP) and related implementing regulations.[14] The process, which begins with digital tracking, followed by arrest, search, and seizure, reflects law enforcement officials' use of an information technology-based approach to combating digital crime.

However, the author also notes that arrests without prior summons, while permissible under certain circumstances (e.g., when caught red-handed or when there is a risk of escape), must still be carried out with extreme caution and accompanied by a valid

arrest warrant. This is crucial to uphold the principles of legality and accountability of the authorities, as well as to avoid potential violations of the suspect's human rights.

2. Obstacles Faced by the Police in Determining Suspects in Gambling Promotion Cases Through Information Technology (Online).

The obstacles faced by the police in naming suspects in cases of online gambling promotion are complex and encompass various aspects, including technical, legal, and administrative aspects. The following is a study conducted by the South Sulawesi Regional Police, which identified the obstacles encountered:[15]

1) Technical Challenges

Technically, the main challenge law enforcement officials face in prosecuting online gambling crimes committed through social media and instant messaging apps is limited access to encrypted communication data. Currently, most digital communication apps, such as WhatsApp, Telegram, and Signal, use end-to-end encryption, which ensures that only the sender and recipient can read the contents of a conversation. Therefore, third parties, including law enforcement officials, cannot access the contents of these messages, even with investigative authorization, except through direct collaboration with the service provider. According to Brigadier Gihon Life Purba of Sub-Directorate V of the Cyber Crime Investigation Unit of the South Sulawesi Regional Police, this encryption system poses a serious obstacle to law enforcement because criminals, including online gambling promoters, are increasingly aware of legal loopholes and are exploiting platforms that are legally and technically difficult to access. He emphasized that in many cases, investigators face difficulties in obtaining relevant communication content as evidence because platform providers are generally located overseas and bound by their respective countries' privacy policies. Brigadier Gihon also added that although the authorities have the technical capability to conduct digital forensics, without official and legitimate international cooperation with application providers, law enforcement can only operate on open-source intelligence, thus being unable to penetrate the perpetrator's personal communication system.

2) The identity of the perpetrator is easily disguised

One of the serious obstacles in uncovering online gambling promotion cases through information technology is the perpetrators' ability to easily disguise their digital identities. Perpetrators typically use fake social media accounts or fictitious identities created to avoid detection. They also utilize Virtual Private Network (VPN) technology or proxy servers to conceal their real IP addresses and geographic locations. As a result, the initial identification and tracking of perpetrators becomes extremely complex and time-consuming. According to Brigadier General Muhammad Aksan, a non-commissioned officer in the Sub-Directorate 5 Tipidcyber Unit of the South Sulawesi Regional Police's Criminal Investigation Directorate, the use of fake digital identities and VPNs is a common tactic in cybercrime cases, including online gambling promotion. He explained that perpetrators frequently switch accounts and use multiple devices to disguise their digital footprints. This requires investigators to conduct in-depth digital analysis, requiring considerable time and resources to trace the perpetrators' chain of activity back to the source. Aksan also added that in some cases, perpetrators even use other people's identities without the owner's knowledge to create promotional social media accounts, leading to misidentification early in the

investigation. Therefore, every step in the search process must be carried out carefully and based on strong digital forensic data verification.

3) Lack of public participation

One significant non-technical obstacle in handling online gambling promotion cases is the lack of active public participation in reporting illegal content, particularly content containing elements of online gambling promotion. This lack of legal awareness among the public means that much harmful content continues to circulate in the digital space without being quickly detected by law enforcement. This content often goes viral and is accessed by many people before finally receiving the attention of authorities through monitoring or limited reporting. According to Brigadier General Muhammad Aksan, a non-commissioned officer in the Cyber Crimes Unit of the South Sulawesi Regional Police's Criminal Investigation Directorate, the lack of public reporting is one factor that delays law enforcement intervention in such cases. He explained that success in eradicating online gambling promotion practices depends heavily on public participation as initial monitors in the digital space, given the limited personnel and reach of the police in monitoring all social media platforms in real time. Aksan added that many people are aware of such content but choose to remain silent because they consider it a private matter or do not understand the legal consequences.

This demonstrates the need to improve digital and legal literacy in the community, particularly regarding the dangers and legal consequences of online gambling and the activities that support it, including its promotion. The author believes that preventive strategies such as legal outreach in schools, communities, and digital media must be intensified, along with the provision of faster, easier, and more integrated public reporting channels with law enforcement. Thus, the public will not only become objects of legal protection but also active subjects in maintaining a healthy digital space free from cybercrime.

D. CONCLUSION

The legal procedure for naming a suspect for promoting a website in an online gambling case at the South Sulawesi Regional Police involved investigation, inquiry, gathering valid evidence, and examining witnesses. After gathering at least two pieces of evidence sufficient to meet the Criminal Procedure Code (KUHAP), investigators named the perpetrator as a suspect. This law enforcement was carried out carefully, considering that perpetrators often disguise their digital identities through fake accounts and the use of VPNs. Obstacles faced by the South Sulawesi Regional Police in naming suspects for promoting online gambling cases through information technology include difficulty in tracking the perpetrator's identity due to the use of fake social media accounts, VPNs, and proxies that obscure digital footprints. Furthermore, technical obstacles include limited access to encrypted communication data and a lack of public participation in reporting online gambling promotion cases. The South Sulawesi Regional Police are advised to increase the capacity of investigators in the field of cybercrime through technical training, the formation of a dedicated cyber team, and strengthening cooperation with the Ministry of Communication and Information Technology and digital platform providers to facilitate the identification of perpetrators. Furthermore, technological equipment and support systems are needed to overcome technical obstacles in handling online gambling promotion cases

REFERENCE

[1] D. Izza, "Transaksi Terlarang Dalam Ekonomi Syariah," *J. Keadaban*, vol. 3, no. 2, pp. 26–35, 2021.

[2] M. J. B. . Tendean, D. Rumimpunu, and D. E. Rondonuwu, "Pertanggungjawaban Pidana Terhadap Promosi Iklan Judi Online Di Media Sosial," *Lex Priv.*, vol. 16, no. 1, 2025, [Online]. Available: http://repository.upbatam.ac.id/2752/1/Cover%2520s.d%25

[3] Firmansyah Firmansyah, "Kebijakan Hukum Pidana mengenai Kejahatan Judi Online (Cyber Gambling) di Indonesia," *J. Hukum, Polit. Dan Ilmu Sos.*, vol. 3, no. 4, pp. 310–318, 2024, doi: 10.55606/jhpis.v3i4.4473.

[4] P. R. N. 24/Menkes/2022, "PENGGUNAAN SISTEM GACHA DALAM GAME ONLINE DILIHAT DARI PERSPEKTIF HUKUM PIDANA," no. 8.5.2017, pp. 2003–2005, 2022.

[5] C. A. Millenia and A. C. Cindrapole, "ISLAMIC LEGAL ANALYSIS ON SUSPECTS," pp. 1–12, 1945.

[6] A. A. Siahaan, M. Y. Lubis, and M. A. Sahlepi, "Analisis Yuridis Penegakan Hukum terhadap Pelaku Tindak Pidana Perdagangan Orang Lintas Negara," *J. Ilm. Metadata*, vol. 4, no. 3, pp. 1–23, 2022.

[7] D. Al Mustaqim, F. Abdul Hakim, H. Atfalina, and A. Fatakh, "Peran Media Sosial Sebagai Sarana Partisipasi Warganet Dalam Mewujudukan Keadilan dan Akuntabilitas Penegakan Hukum di Indonesia," *J. Multidiscip. Res. Dev.*, vol. 1, no. 1, pp. 53–66, 2024, doi: 10.56916/jmrd.v1i1.655.

[8] N. Qamar *et al.*, "Metode Penelitian Hukum (Legal Research Methods)," no. December, p. 176, 2017.

[9] sembiring juhardi syahputra eko, novianty lily, "KEBIJAKAN PENEGAKAN HUKUM PIDANA DALAM RANGKA PENANGGULANGAN PERJUDIAN ONLINE," *J. Eng. Res.*, vol. 10, no. 1, pp. 35–45, 2023.

[10] P. Magister, *METODE KEPOLISIAN DALAM PENEGAKAN HUKUM TERHADAP MENINGKATNYA AKTIVITAS PERJUDIAN ONLINE*. 2024.

[11] Reza Ditya Kesuma, "Penegakan Hukum Perjudian Online di Indonesia: Tantangandan Solusi," *J. Exact J. Excell. Acad. Community*, vol. 1, no. 1, p. 2023, 2023.

[12] D. R. Anggraeni and M. Salsabila, "Analisis Yuridis Peran Digital Forensik Dalam Pembuktian Tindak Pidana di Indonesia," *Media Huk. Indones.*, vol. 2, no. 2, pp. 593–600, 2024.

[13] N. Citra Dewi, T. Sutabri, and F. Putrawansyah, "Analisis Penyadapan Pada Telegram Dengan Network Forensic," *JIKO (Jurnal Inform. dan Komputer)*, vol. 7, no. 2, p. 183, 2023, doi: 10.26798/jiko.v7i2.789.

[14] N. Nim and D. Kurniawan, "UPAYA REPRESIF KEPOLISIAN DALAM MEMBERANTAS AKTIVITAS JUDI ONLINE (Studi Penelitian di Polres Wonosobo) TESIS," 2024.

[15] I. Irnayanti, M. Pawennei, and K. Ahmad, "Analisis Yuridis Terhadap Tindak Pidana Penipuan Di Wilayah Hukum Kepolisian Daerah Sulawesi Selatan," *J. Lex Theory*, vol. 5, 2024, [Online]. Available: http://www.pasca-umi.ac.id/index.php/jlt/article/download/1679/1958