

Legal Analysis of Investigations into Pornographic Video Distribution on Social Media: A Study of the Maluku Regional Police Cyber Unit

Riski Patti Waleulu 

Islamic Criminal Law Study Program, Faculty of Sharia, UIN Abdul Muthalib Sangadji
Jl. Dr. H. Tarmizi Taher Jalan Kebun Cengkeh, Batu Merah, Kec. Sirimau, 97128, Indonesia
E-mail Correspondence Author: [*waleuluriski653@gmail.com](mailto:waleuluriski653@gmail.com) 

Article Info

Article history:

Received: April 10, 2026

Revised: May 20, 2026

Accepted: June 15, 2026

Keywords:

Distribution of Pornographic Videos,
Maluku Regional Police,
Social Media.

ABSTRACT

This study aims to examine the Maluku Regional Police's investigation into the crime of distributing pornographic videos and identifying perpetrators of the distribution of pornographic videos on social media. This research method is field research, utilizing field data as the primary source, such as observational interviews and documentation. It also analyzes the legal framework related to the investigation into the crime of distributing pornographic videos and identifying perpetrators of the distribution of pornographic videos on social media conducted by the Maluku Regional Police. The results indicate that the investigation into the crime of distributing pornographic videos on social media begins with receiving a report from the public, which serves as the basis for the police to identify the source of the video and collect digital evidence. All of these stages are regulated by various laws and regulations, such as the Criminal Procedure Code (KUHP), the Electronic Information and Transactions Law (UU ITE), and the Criminal Code (KUHP). The research results also show that the determination of perpetrators of the distribution of pornographic videos on social media by the Maluku Regional Police was carried out by identifying initial evidence in the form of videos, photos, or links that were distributed, as well as securing the URL of the social media account profile as a basis for tracking and determining the suspect based on the fulfillment of two valid pieces of evidence, accompanied by legal action in the form of arrest, examination, and detention. To prevent the perpetrator from repeating his actions, the police secured the electronic devices and social media accounts used.

 <https://doi.org/10.30598/pustakahukumv1i1pp01-08>



This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution-ShareAlike 4.0 International License](#).

1. INTRODUCTION

According to Article 1 paragraph (3) of the 1945 Constitution (UUD NRI 1945), Indonesia is a state based on law. The 1945 Constitution advised Indonesia's founding fathers to establish a state based on law, not power. To ensure order, security, justice, and prosperity for its people, Indonesia establishes law as the highest authority. Therefore, every action taken by Indonesian citizens is based on law [1]. The current development of information technology has brought humanity into an era of highly liberated globalization, which has had various consequences, both positive and negative [2]. With the emergence of internet services, technological globalization has transformed the world into the cyber era. The emergence of these services has created cyberspace, a virtual world that offers various conveniences [3]. However, technological advances, including the direct development of the internet, have given rise to a variety of new legal issues. One type of crime exploiting the internet through social media is online pornography, also known as cyberpornography. This is the dissemination of immoral content (pornography) accessible to the public using the internet. On social media, cyberpornographic content typically consists of pornographic videos, moving animations, and erotic images [4]. According to Soerjono Soekanto, technological advances will go hand in hand with the emergence of changes in society. These changes in society can affect social values, social norms, behavioral patterns, organizations, and the structure of social institutions [5]. To prevent crimes occurring in the field of Information Technology and Electronic Transactions, the Indonesian government issued Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, commonly referred to as the ITE Law. However, in reality, crimes in the ITE sector still occur frequently, such as defamation, cyber network destruction (hacking) and the distribution of content that violates moral values, such as pornographic images or videos. Regarding investigations, the Criminal Procedure Code defines an investigation as a series of investigative actions, in accordance with the methods stipulated in this law, to seek and collect evidence that sheds light on the crime that has occurred and to identify the suspect. As explained in the discussion of general provisions, Article 1, paragraphs 1 and 2 define an investigation, stating that investigators are carried out by National Police officers or "certain" civil servants granted special authority by law [6]. The offense punishable by Article 282 is broadcasting, displaying, creating, offering, or otherwise transmitting writings, images, or objects that violate morality or are pornographic. The crime of pornography is regulated in Law Number 1 of 1960 concerning the Criminal Code (KUHP) and more specifically in Law Number 44 of 2008 concerning Pornography (UUP). However, due to changes in the method, with the use of electronic media as a means of distribution, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) was enacted [7]. In Maluku, particularly on Ambon Island, several cases have recently emerged, starting with the circulation of viral videos containing elements that violate morality, such as videos circulating on social media with titles such as "ice cubes," "hot water," "Chinese graves," and most recently, "grandpa and young lady." The cases mentioned above raise questions among the public regarding the widespread distribution of pornographic videos on social media, and the process by which the Maluku Regional Police apply criminal sanctions to accounts involved in these distributions. This becomes interesting to examine further.

Based on initial observations, the Maluku Regional Police, in their efforts to handle cases of pornographic videos on social media, are in accordance with the mandate of the law, namely the Electronic Information and Transactions (ITE) Law and the Pornography Law. The investigation and prosecution of these cases are conducted by the Maluku Regional Police's cyber division. They first receive reports from victims and find pornographic videos circulating on social media in violation of the ITE Law and the Pornography Law. We, as investigators, first consult with our superiors regarding the issue. After that, our superiors appoint individuals to handle the case. The appointed individuals then carry out administrative processes related to the report and the pornography case. We then conduct interviews with experts in the field of ITE, and we examine witnesses and evidence. From the results of the witness examination, a case title is carried out to determine the suspect, if everything has been done starting from the statements of the victim, witnesses, and evidence, then we will summon the perpetrator, the suspect, If it has been determined then we will carry out detention, as for there is an error then an extension will be requested by the investigator at the Prosecutor and the court, Because what can decide the sentence period is determined by the court, which usually occurs when the error is in virtual evidence, therefore we carry out a digital forensic examination at the center and sometimes also in Makassar. Some of the cases handled by the Maluku Regional Police involve individuals aged 20-40 years. The perpetrators we handle are not only native to Maluku but also from outside Maluku. The number of cases in the past year, 2023-2024, was approximately 10-15, a significant decrease compared to the previous year. Certainly, there are challenges when handling cases of pornographic video distribution on social media, such as perpetrators using fake accounts, which makes it difficult for experts and investigators to investigate [8]. The investigation was conducted to obtain evidence of the criminal act of distributing pornographic videos on social media. To obtain this evidence, a laboratory examination of the case under investigation is required, along with a legal opinion from a professional expert.

2. METHOD

This study employed a qualitative field research design to explore the legal enforcement of cases involving the dissemination of pornographic videos through social media in Indonesia. The research was conducted between October and December 2024 at the Cybercrime Unit (Sub-Directorate V Cyber) of the Maluku Regional Police (Polda Maluku), Ambon, Indonesia, as the institution responsible for investigating cybercrime cases. Primary data were collected through semi-structured interviews with three purposively selected law enforcement officers who possess direct experience in handling cybercrime investigations related to pornography offenses, while secondary data were obtained from statutory regulations, official reports, case-related documents, academic journals, books, and other relevant legal literature. Data were collected using three complementary techniques, namely direct observation of institutional practices and publicly accessible social media content, in-depth interviews with key informants, and documentation of legal and institutional records. The collected data were analyzed using the interactive analysis model developed by Miles and Huberman, which includes data reduction, data display, and conclusion drawing and verification. To enhance the credibility and trustworthiness of the findings, methodological triangulation was applied by comparing evidence obtained from interviews, observations, and documentary sources, thereby ensuring the consistency and validity of the research results.

3. RESULTS AND DISCUSSION

3.1 Overview of the Research Setting

The Cybercrime Unit (Sub-Directorate V Cyber) of the Maluku Regional Police (Polda Maluku) serves as the primary law enforcement institution responsible for investigating cybercrime cases within Maluku Province, including the dissemination of pornographic content through digital platforms. The institution operates under the Directorate of Special Criminal Investigation (Ditreskrimsus) and is responsible for conducting cybercrime investigations, collecting digital evidence, performing digital forensic examinations, and coordinating with relevant national agencies in enforcing cyber law [9]. As a regional police institution, Polda Maluku has jurisdiction over all regencies and municipalities within Maluku Province and plays a significant role in maintaining public order, preventing cybercrime, and enforcing criminal law in cyberspace [10]. The organizational structure, statutory authority, and investigative responsibilities of the Cybercrime Unit therefore provide an appropriate institutional context for examining the implementation of criminal investigations involving the dissemination of pornographic content through social media.

3.2 Investigation Process of the Dissemination of Pornographic Videos through Social Media

The findings indicate that criminal investigations into the dissemination of pornographic videos through social media commence upon receiving a report or complaint from victims or members of the public. The report serves as the legal basis for investigators to conduct preliminary examinations, identify the source of the content, and secure digital evidence before initiating a formal investigation. According to interviews with investigators from the Cybercrime Unit of the Maluku Regional Police, the most significant challenges include identifying anonymous perpetrators, tracing fake social media accounts, and collecting electronic evidence distributed across multiple digital platforms [11].

The investigation process subsequently proceeds through several procedural stages, including preliminary inquiry, formal investigation, collection of electronic evidence, witness examination, suspect interrogation, digital forensic analysis, detention where necessary, prosecution, and judicial proceedings. Throughout these stages, investigators rely extensively on electronic evidence, such as screenshots, Uniform Resource Locator (URL) profiles, Internet Protocol (IP) addresses, digital communication records, and forensic examinations of electronic devices [12]. These procedures are carried out in accordance with the Indonesian Criminal Procedure Code (KUHAP), the Electronic Information and Transactions Law (Law No. 11 of 2008 as amended by Law No. 1 of 2024), and Law No. 44 of 2008 concerning Pornography.

The interview findings further reveal that effective cybercrime investigations require close cooperation between regional police investigators, the National Police Headquarters (Bareskrim Polri), digital forensic experts, and social media service providers. Such collaboration is particularly necessary when perpetrators operate anonymous accounts or are located outside the jurisdiction of the Maluku Regional Police. These findings demonstrate that technological capability and inter-agency cooperation have become essential elements in enforcing criminal law against online pornography [13].

These findings are consistent with Gunawan et al. (2021), who argued that Article 27 paragraph (1) of the Electronic Information and Transactions Law constitutes the

principal legal foundation for prosecuting individuals who distribute electronic content containing pornography. Likewise, Putra and Rizqia (2019) found that limitations in digital evidence collection and technological resources remain major obstacles to effective cybercrime investigations. The present study extends previous research by demonstrating that investigators at the Maluku Regional Police increasingly rely on digital forensic techniques and institutional coordination to establish criminal responsibility in cases involving the dissemination of pornographic videos through social media [14].

3.3 Challenges in Determining Suspects in Pornography-Related Cybercrime Cases

The study further revealed several practical challenges in determining suspects involved in the dissemination of pornographic videos through social media. Investigators explained that the identification of suspects largely depends on the availability of at least two legally admissible forms of evidence as required under Article 184 of the Indonesian Criminal Procedure Code [15]. In cases involving anonymous or fake social media accounts, investigators first secure the Uniform Resource Locator (URL), digital profile information, and electronic communication records before coordinating with the National Police Headquarters and relevant digital service providers to trace the identity of account owners [16]. Digital forensic examination, witness testimony, expert opinions, screenshots, electronic documents, and device examinations constitute the principal sources of evidence used during investigations [17]. Another significant obstacle concerns victims who withdraw complaints before the investigation is completed, perpetrators located outside the jurisdiction of the Maluku Regional Police, and delays in obtaining electronic data from international digital platforms. These factors often prolong investigative procedures and complicate the establishment of criminal liability. Nevertheless, investigators reported that technological advancements in digital forensics, combined with institutional cooperation among law enforcement agencies and government institutions, have substantially improved their ability to identify offenders and secure legally admissible electronic evidence [18]. The findings corroborate previous research indicating that the effectiveness of cybercrime law enforcement depends not only on the existence of adequate legal provisions but also on technological capability, institutional cooperation, public participation, and digital forensic capacity [19]. While Indonesian legislation provides comprehensive legal instruments for prosecuting online pornography, practical implementation continues to face technical and procedural challenges. Therefore, strengthening digital forensic infrastructure, enhancing cooperation with global social media providers, and improving investigators' technical competencies are essential to increasing the effectiveness of criminal investigations involving the dissemination of pornographic content through social media [20].

4. CONCLUSION

This study concludes that the investigation of the dissemination of pornographic videos through social media by the Cybercrime Unit (Sub-Directorate V Cyber) of the Maluku Regional Police has generally been conducted in accordance with the Indonesian legal framework, particularly the Indonesian Criminal Procedure Code (KUHAP), Law No. 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions (ITE) Law, Law No. 44 of 2008 concerning Pornography, and other relevant criminal law provisions. The investigation process begins with receiving reports or complaints from the public, followed by preliminary inquiries,

formal investigations, the collection and examination of digital evidence, witness and suspect examinations, forensic analysis of electronic devices, and judicial proceedings where sufficient evidence is established. The findings demonstrate that digital evidence plays a central role in establishing criminal liability in cybercrime cases involving pornographic content. However, investigators continue to face substantial practical challenges, including difficulties in identifying anonymous perpetrators, tracing fake social media accounts, obtaining electronic evidence distributed across multiple digital platforms, and securing cooperation from international social media service providers. The determination of suspects is further constrained by the legal requirement that investigators possess at least two legally admissible forms of evidence before criminal charges can be formally initiated. Additional obstacles arise when victims withdraw their complaints, perpetrators reside outside the jurisdiction of the Maluku Regional Police, or electronic data cannot be obtained promptly because of cross-border legal and technical limitations. Despite these challenges, the study indicates that technological advancements in digital forensic investigation, improved institutional coordination with the National Police Headquarters and other government agencies, and the increasing use of digital investigative techniques have significantly enhanced the effectiveness of cybercrime investigations. These findings suggest that the effectiveness of law enforcement in combating the dissemination of pornographic content on social media depends not only on the adequacy of existing legal regulations but also on the availability of advanced digital forensic infrastructure, competent investigators, institutional collaboration, and public participation in reporting cybercrime. Accordingly, strengthening the technical capacity of cyber investigators through continuous professional training, improving cooperation with domestic and international digital platform providers, enhancing inter-agency coordination, promoting digital literacy and legal awareness among the public, and establishing more effective procedures for securing and preserving electronic evidence are essential measures for improving future investigations. Collectively, these efforts will contribute to a more effective, accountable, and technologically responsive criminal justice system capable of addressing the growing complexity of cybercrime and protecting society from the harmful consequences of the online dissemination of pornographic content.

Acknowledgments

The authors sincerely thank the Cybercrime Unit (Sub-Directorate V Cyber) of the Maluku Regional Police (Polda Maluku) for granting permission to conduct this research and for providing valuable information during the interview process. The authors also express their appreciation to all research participants who voluntarily shared their knowledge and professional experience, which significantly contributed to the completion of this study.

Funding Information

The authors state that no external funding was received for this research.

Author Contributions Statement

First Author: Conceptualization, methodology, investigation, data curation, formal analysis, writing original draft, and visualization. **Second Author:** Supervision, methodology, validation, writing review and editing. **Third Author:** Resources, project administration, validation, and writing review and editing. All authors discussed the findings, reviewed the manuscript critically, approved the final version of the manuscript, and agreed to be accountable for all aspects of the work.

Conflict of Interest Statement

The authors declare that they have no known competing financial interests, personal relationships, or professional affiliations that could have appeared to influence the work reported in this paper. The authors state no conflict of interest.

Informed Consent

Written informed consent was obtained from all individuals who voluntarily participated in this study prior to data collection. All participants were informed about the purpose of the research, the voluntary nature of their participation, and the confidentiality of the information they provided.

Ethical Approval

The research involving human participants was conducted in accordance with applicable national regulations and institutional ethical principles. Participation in this study was voluntary, and confidentiality and anonymity were maintained throughout the research process. Formal permission to conduct the research was obtained from the Cybercrime Unit (Sub-Directorate V Cyber) of the Maluku Regional Police.

Data Availability

The data supporting the findings of this study are available from the corresponding author upon reasonable request. The data are not publicly available because they contain information that could compromise the privacy and confidentiality of the research participants and law enforcement investigations.

Declaration of Generative AI and AI-assisted Technologies

Generative AI tools were used solely for language refinement and formatting of the manuscript. The study design, data collection, analysis, interpretation of results, and conclusions were conducted entirely by the authors. The authors take full responsibility for the scientific content of this manuscript.

REFERENCES

- [1] Renardi, A. (2023). "Legal Analysis of Law Enforcement of the Criminal Act of Distributing Pornography by Uploading Videos on Social Media" (Study of Decision Number 2661/Pid. Sus/2020/Pn. Mdn) (Doctoral Dissertation, Faculty of Law, Islamic University of North Sumatra).
- [2] Markuat, M. (2022). "Legal Analysis of the Criminal Act of Disseminating Pornographic Photos/Videos in Electronic Media" (Study of Decision Number: 902/Pid. B/2020/Pn Jkt. Pst). Khatulistiwa: Journal of Education and Social Humanities, 2(2), 27-43.
- [3] Markuat, M. (2022). "Legal Analysis of the Criminal Act of Disseminating Pornographic Photos/Videos in Electronic Media" (Study of Decision Number: 902/Pid. B/2020/Pn Jkt. Pst). Khatulistiwa: Journal of Education and Social Humanities, 2(2), 27-43.
- [4] Mala Mutiara Raiz, 2021, "Criminological Review of Pornography Crimes Through Video Calls (Case Study in Makassar City 2018-2020)", Thesis, Bachelor of Laws, Faculty of Law, Hasanuddin University Makassar, p. 2
- [5] Soerjono Soekanto, Principles of Legal Sociology, Rajawali Pers, Jakarta, 2014, pp. 87-88
- [6] M. Yahya Harahap, Discussion of Problems and Application of the Criminal Procedure Code (investigation and prosecution), Sinar Grafika, Jakarta, 2008, p. 109.
- [7] Erinda Sinaga, "Review of the Responsibility of Perpetrators of Pornography Crimes According to Law Number 44 of 2008 Concerning Pornography", Journal of Legal Studies, Vol. 8 No. 4, University of Riau, 2014.
- [8] Initial observation: Arter Siaranamor, assistant investigator of the Cyber Crimes Sub-Directorate, Directorate of Special Criminal Investigation, Maluku Regional Police. August 26, 2024

- [9] Indonesian National Police, DIT RESKRIMSUS – Tugas dan Fungsi, Official Website of the Indonesian National Police, available at: DIT RESKRIMSUS – Tugas dan Fungsi (accessed 15 July 2026).
- [10] Maluku Regional Police, Amankan Pilkada, Polda Maluku Patroli Cyber, Takedown Konten Ujaran Kebencian di Medsos, Official Website of Polda Maluku, 27 September 2024, available at: Official Polda Maluku News (accessed 15 July 2026).
- [11] Interview with Arter Siaranor, Assistant Investigator, Sub-Directorate V Cyber, Directorate of Special Criminal Investigation, Maluku Regional Police, Ambon, Indonesia, 2024.
- [12] Law No. 8 of 1981 concerning the Indonesian Criminal Procedure Code (KUHP); Law No. 11 of 2008 concerning Electronic Information and Transactions as amended by Law No. 1 of 2024; and Law No. 44 of 2008 concerning Pornography.
- [13] Interview with Arifiyanto Kayat, S.H., Police Officer, Sub-Directorate V Cyber, Maluku Regional Police, Ambon, Indonesia, 2024.
- [14] Gunawan et al., "Law Enforcement Against the Distribution of Pornographic Content Through Electronic Media," 2021; Putra & Rizqia, "Challenges in Cyberporn Law Enforcement in Indonesia," 2019.
- [15] Law No. 8 of 1981 concerning the Indonesian Criminal Procedure Code (KUHP), Article 184, which regulates the legally recognized forms of evidence in criminal proceedings.
- [16] Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), particularly provisions governing electronic information, electronic documents, and electronic evidence as admissible evidence in criminal proceedings.
- [17] Edmon Makarim, Pengantar Hukum Telematika: Suatu Kompilasi Kajian (Jakarta: PT RajaGrafindo Persada, 2005), pp. 235–248.
- [18] Interview with Arter Siaranor, Assistant Investigator, Sub-Directorate V Cyber, Directorate of Special Criminal Investigation, Maluku Regional Police, Ambon, Indonesia, conducted on October 2024.
- [19] Barda Nawawi Arief, Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan (Jakarta: Kencana, 2018), pp. 357–366.
- [20] UNODC (United Nations Office on Drugs and Crime), Comprehensive Study on Cybercrime (Vienna: United Nations, 2013), pp. 215–226.