HORIZON PUBLIC LEGAL STUDIES
Vol 2 Issue 1 Tahun 2025
Doi : https://doi.org/10.56087/hegels.v2i1.1324

COLD-BLOODED CYBER EXTORTION TRAP: The Method of Distributing Immoral Content as a Criminal Weapon of Threats on Social Media

Surya Wirawan[1], Nur Fadhilah Mappaselleng[2], Dwi Handayani[3]

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

Surel Koresponden: ardeliarahmadani11@gmail.com

Abstrak: Penelitian ini bertujuan untuk menentukan dan menganalisis proses investigasi tindak pidana pengancaman dan pemerasan melalui media sosial serta mengidentifikasi faktor-faktor penghambat dalam investigasi tindak pidana pengancaman dan pemerasan melalui media sosial, khususnya yang melibatkan penyebaran konten immoral. Penelitian ini menggunakan metode penelitian empiris. Teknik pengumpulan data meliputi wawancara dan dokumentasi. Penelitian ini dilakukan di Makassar, khususnya di Markas Besar Kepolisian Daerah Sulawesi Selatan. Hasil penelitian penulis menunjukkan bahwa proses investigasi tindak pidana pengancaman dengan pemerasan sama dengan penanganan kejahatan umum lainnya jika laporan diterima maka diterbitkan surat perintah investigasi dan SP2HPA1 (Pemberitahuan Kemajuan Laporan Hasil Penelitian). Hasil investigasi menemukan setidaknya 2 barang bukti awal yang cukup sesuai dengan ketentuan Pasal 184 KUHP maka statusnya akan dinaikkan dari tahap pendahuluan ke tahap pendahuluan dan diterbitkan SP2HP A3 (Pemberitahuan Hasil Investigasi). Namun, jika hasil penyelidikan kasus yang dilaporkan bukan kasus pidana atau tidak memenuhi ketentuan Pasal 184 KUHP, maka penyelidikan harus dihentikan dan diterbitkan SP2HP A2 (Pemberitahuan Perkembangan Hasil Penyelidikan) atau biasanya penyelidikan dihentikan. Faktor penghambat dalam proses penyelidikan terhadap tersangka yang melakukan tindak pidana pengancaman dan pemerasan melalui media sosial antara lain terkadang pihak pelapor tidak kooperatif, bukti telah dihapus sehingga proses pelacakan digital menjadi lebih rumit dan panjang, dan pelaku biasanya berada di luar yurisdiksi Kepolisian Daerah Sulawesi Selatan dan seringkali terdapat kekurangan saksi dan bukti. Rekomendasi penulis adalah agar kepolisian meningkatkan kerja sama dalam menyelesaikan kasus pidana, baik dengan instansi terkait maupun dengan masyarakat. Selain itu, diperlukan juga pendidikan masyarakat yang komprehensif mengenai pentingnya sikap kooperatif dalam berurusan dengan hukum untuk mempermudah penyelidikan dan penanganan kasus. Masyarakat juga perlu meningkatkan kesadaran akan keamanan media elektronik dan berpartisipasi dalam melaporkan kejahatan siber kepada polisi. Petugas penegak hukum juga perlu dilengkapi dengan alat yang memadai dan memperkuat koordinasi serta kerja sama antara pemerintah, petugas penegak hukum, dan masyarakat. Dengan demikian, langkah-langkah ini diharapkan dapat meningkatkan efektivitas penegakan hukum dan mengurangi hambatan dalam mengatasi penyebaran konten immoral melalui media elektronik.

Kata Kunci: Investigasi, Kejahatan, Pemerasan, Media Sosial

***Abstract**: This study aims to determine and analyze the investigation process for criminal acts of threats and extortion via social media and to identify the inhibiting factors in the investigation of*

criminal acts of threats and extortion via social media, particularly involving the distribution of immoral content. This study employed empirical research methods. Data collection techniques included interviews and documentation. The study was conducted in Makassar, specifically at the South Sulawesi Regional Police Headquarters. The results of the author's research are that the process of investigating criminal acts of threats with extortion is the same as handling other general crimes if the report is received then an investigation warrant and SP2HPA1 (Notification of the progress of the report research results) are issued. The results of the investigation find at least 2 initial pieces of evidence that are sufficient in accordance with the provisions of Article 184 of the Criminal Procedure Code then the status will be raised from the preliminary stage to the preliminary stage and the issuance of SP2HP A3 (Notification of Investigation Results) is issued. However, if the results of the investigation of the reported case are not a criminal case or do not meet the provisions of Article 184 of the Criminal Procedure Code then the investigation must be stopped and the issuance of SP2HP A2 (Notification of the Progress of Investigation Results) or usually the investigation is stopped. The inhibiting factors in the investigation process against suspects who commit criminal acts of threats and extortion through social media include sometimes the reported party is not cooperative, evidence has been deleted which results in the digital tracking process becoming more complicated and long, and the perpetrator is usually outside the jurisdiction of the South Sulawesi Regional Police and there is often a lack of witnesses and evidence. The author's recommendation is that the police should increase cooperation in resolving criminal cases, both with related agencies and with the public. There is also the need for comprehensive public education regarding the importance of a cooperative attitude when dealing with the law to facilitate investigations and handling of a case. The public also needs to increase awareness of electronic media security and participate in reporting cybercrime to the police. Law enforcement officers also need to be equipped with adequate tools and strengthen coordination and cooperation between the government, law enforcement officers, and the public. Thus, these steps are expected to increase the effectiveness of law enforcement and reduce obstacles in overcoming the spread of immoral content through electronic media.

Keywords: *Investigation, Crime, Blackmail, Social Media*

A. INTRODUCTION

The lifestyle and mindset of today's society are greatly influenced by technological advances in the era of globalization.[1] The presence of communication and information technology aims to simplify various activities and meet human needs. Electronic media is one of the technological innovations that acts as an information channel that is able to reach people in various regions widely, thus creating a society that is easier and freer in activities and creativity, as well as changing the way people view communication, socializing, and doing business. In human life as social beings, of course, requires interaction with other humans, interactions that

are often carried out in daily life certainly provide various influences, including positive and negative influences.[2] The negative influence of interaction often gives rise to a crime, which generally in a crime there are two parties that are interconnected, namely the perpetrator and the victim of the crime.[3] In reality, a crime would not occur without the perpetrator and the victim of the crime. Each is a component of an interaction (absolute), the result of which is a crime. Technological progress at this time has developed so rapidly that it has caused a world without boundaries, directly or indirectly changing the lifestyle of society.[4] Due to technological advancements in society, crimes are no longer committed through conventional means but are now utilizing advances in information technology, such as fraud, defamation, extortion, and threats by misusing technological advancements. This proves that technological advancements are used as opportunities to commit cybercrime.[5] Communication and information technology through social media is seen to have developed extraordinarily. However, technological advancements through the development of the Internet have directly created various new legal issues.[6] One type of crime that is increasingly exploiting the internet through social media is pornography, where most perpetrators carry out threats or blackmail through immoral content, better known as cyber pornography, which involves the distribution of indecent content so that it can be accessed by the public using the internet network. The content of cyber pornography on social media usually takes the form of pornographic videos, moving animations, and erotic images.[7] To overcome the spread of cyber pornography on social media such as Twitter, Telegram, Facebook, Line, and other platforms, strict legal sanctions are needed to provide a deterrent effect for violators who distribute immoral videos, supported by strong evidence. This evidence plays a crucial role in processing cyber pornography cases in court, considering that social media has been misused by certain groups to disseminate pornographic products that have a negative impact on society. Technology will continue to advance over time.[8] Therefore, it is possible that the internet can also increase social problems in society, namely the emergence of internet injustice, which we often call cybercrime in the world of cyberspace (the internet world). The ASEAN Declaration on December 20, 1997 in Manila has analyzed various types of crimes, including cybercrime, namely:

1. Cyber Terrorism (National Police Agency of Japan (NPA))

2. Cyber Pornography
3. Cyber Harassment
4. Cyber Stalking
5. Hacking
6. Carding (credit card fraud)

The misuse or negative impact of advances in information technology through computerized systems and internet networks is known as cybercrime. One of the most common cybercrimes in our society today is the crime of morality, namely cyber pornography. Cyber Pornography itself can perhaps be interpreted as the distribution of pornographic content via the internet. Article 281-283 of the Criminal Code, one of which (Article 282) regulates crimes against morality which include "Distribution or dissemination of content in the form of images, writings or objects containing immoral content in public." Related to criminal regulations on morality are also contained in Law Number 44 of 2008 concerning Pornography. The regulations were expanded with the existence of Law Number 19 of 2016 Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions ("ITE").[9] Provisions governing the distribution of immoral content can be seen in Article 27 Paragraph (1) of the ITE Law. This article states: "Any person who intentionally and without the right transmits, accesses, distributes and/or makes available Electronic Information and/or Electronic Documents that contain content that violates morality, 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)."

One of the distribution of immoral content in Indonesia, especially in Makassar City, is increasingly rampant. Quoting from Kompas.com Makassar, there was a case where a perpetrator with the initials ADA (29 years old) was arrested after allegedly blackmailing his ex-girlfriend by threatening to spread the victim's immoral content with the perpetrator. The perpetrator was arrested directly by the Crime and Violence Unit (Jatanras) of the Makassar Police Criminal Investigation Unit at his residence on Jalan Kaccia Tamalate. Where in the content was recorded during a video call and the victim was naked, this was recorded by the perpetrator without the victim's knowledge. From the video, the perpetrator threatened the

victim that if he did not send money amounting to Rp. 10,000,000, the video would be distributed.

B. METHOD

This type of research is Empirical Research, namely research from field data as the main data source, such as interview results and documentation. Empirical research is used to analyze the law that is seen as patterned community behavior in community life. The research location is a place where observations are made to gain knowledge. The author conducted research at the South Sulawesi Regional Police. The selected samples came from: Head of Sub-Directorate 5 of Cyber Crimes, Directorate of Special Criminal Investigation, South Sulawesi Regional Police, primary data used through interview methods with Head of Sub-Directorate 5 of Cyber Crimes, Directorate of Special Criminal Investigation, South Sulawesi Regional Police. Secondary data was carried out as an effort to adjust to the needs of field data. Secondary data was obtained through documents and scientific journals. Data collection techniques were carried out using interview and documentation methods. And Data Analysis was carried out qualitatively by systematically searching and compiling data from interviews and documentation by organizing data and selecting which ones are important and which ones need to be studied and making conclusions so that they are easy to understand.[10]

C. DISCUSSION

1. The Investigation Process of Criminal Acts of Threats and Extortion Through Social Media with the Modus of Distributing Immoral Content.

Investigation is a series of actions by investigators in the case and according to the method regulated in this law to search for and collect evidence that occurred and to find the suspect (Article 1 paragraph 2 of the Criminal Procedure Code). In the investigation carried out by investigators who are officers of the Republic of Indonesia state police or certain civil servants who are given special authority by law to conduct investigations (Article 1 paragraph 1 of the Criminal Procedure Code).[11] Assistant investigators are officers of the Republic of Indonesia state police who because they are given certain authority can carry out investigative duties regulated in this law (Article 1 paragraph 3 of the Criminal Procedure

Code). According to a statement from Bripda Fitah Reski, an investigator at the Cyber Crime Investigation Unit of the South Sulawesi Regional Police, on Friday, July 4, 2025, at 1:00 PM WITA43, he also stated that the series of investigative stages carried out by investigators when handling a crime are:

"Creating an administrative investigation, often called mindik, then searching for facts and gathering witness statements to determine whether a crime has been committed. If there is sufficient evidence, the case is escalated to the investigator's investigation and then issuing a police report to form the basis for the investigation.[12] The stages include summoning witnesses, conducting digital forensics, summoning or naming a suspect. If the suspect is uncooperative, coercive measures will be taken, namely arrest and/or detention, if deemed necessary.[13] The suspect determination stage is based on witness testimony, expert testimony, written evidence or electronic documents, and the suspect's statement, supported by digital forensic results. Once everything is complete, the case file will be submitted to the Prosecutor's Office (JPU) or commonly called P-21, for examination. If the file is complete (P21), the investigator will hand over the suspect and evidence to the public prosecutor for stage 2." In order to prevent uncooperative behavior from perpetrators of threats and extortion, it is necessary to collect data through Cellebrite evidence to find evidence contained on the perpetrator's cell phone.[12] The investigation phase includes the investigation and inquiry phases for handling extortion with threats, namely: Investigation and Inquiry.[12]

Based on the above data, it can be seen that 40 reports regarding threats and extortion within the jurisdiction of the South Sulawesi Regional Police in 2022 were received, with 14 cases resolved through Restorative Justice, and 2 cases resolved through Phase II. In 2023, 20 reports were received, with 7 cases resolved. In 2024, 35 reports were received, 26 cases resolved through RJ, and 6 cases were resolved to the trial stage. The total number of cases of document forgery in the past four years was 95. Cybercrime cases are still rampant due to several factors within society itself. The establishment of Sub-Directorate V Cyber is also inseparable from the rise in cybercrimes. This is due to the increasing advancement of technology.[14]

According to a report from the South Sulawesi Regional Police in 2022, they received numerous reports of approximately 100 cases of Electronic Information and Transactions (ITE).[15] The establishment of the Tipidsiber (Cyber) Division of the South Sulawesi Regional Police's Special Criminal Investigation Directorate aims to allow the police to focus more on handling ITE cases, particularly within the jurisdiction of the South Sulawesi Regional Police. Sub-Directorate V Tipidsiber of the South Sulawesi Regional Police's Special Criminal Investigation Directorate plays a crucial role in carrying out its duties in accordance with applicable regulations. The Cyber Sub-Directorate is tasked with investigating and prosecuting crimes occurring within its jurisdiction.

2. Inhibiting Factors in the Investigation Process of Criminal Acts of Threats and Extortion.

Based on the results of an interview with Kompol Bayu Wicaksono Febrianto S.I.K as Head of Sub-Directorate V Cyber of the South Sulawesi Regional Police on July 29, 2025, conveyed several obstacles faced by investigators during the handling of criminal cases of threats and extortion, namely: "There are several obstacles if there is a case of reporting criminal acts of threats and extortion with the mode of spreading immoral content, namely sometimes the reported party is not cooperative, evidence has been deleted which results in the digital tracking process becoming more complicated and long, the perpetrator is usually outside the jurisdiction of the South Sulawesi Regional Police and there is often a lack of witnesses and evidence. [16]

In general, the author describes several obstacles and/or barriers during the investigation of criminal acts of threats and extortion with the mode of spreading immoral content, namely: 1. Legal factors The legal factors themselves are from the laws and regulations themselves, in this case Law Number 19 of 2016 Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. Perpetrators of violations of morality (cyberporn crimes) can be subject to criminal penalties imprisonment in accordance with the fulfilled criminal elements listed in Article 45 paragraph (1).[9] Examining Article 27 paragraph (1) of the ITE Law, there is a prohibition on committing acts that violate morality which includes the word element of violating morality. The element of "violating morality" in the ITE Law

is problematic because the ITE Law does not include a definition and instructions regarding the element of morality in its explanation. The element that has a content of violating morality in Article 27 Paragraph (1) of the ITE Law which gives rise to various interpretations of a legal norm as an indicator of an error in its formulation.

This weakness in its formulation should be able to be overcome through jurisprudence, because as long as the Judge consistently adheres to a fair decision, in accordance with logic, and in accordance with what the community feels, jurisprudence can be used as a way to overcome deficiencies or errors in the formulation of norms in the law.[1] 2. Law enforcement factors The constraints related to law enforcement in the South Sulawesi Regional Police are the imbalance between the number of police law enforcement officers and the number of cases handled and the number of law enforcement personnel handling criminal cases. Cyberporn. Law enforcement constraints include the limited human resources of the South Sulawesi Regional Police, as most investigators lack information technology expertise and lack a grasp of the rapidly evolving technology.[2] 3. Facilities supporting law enforcement. Inadequate facilities make it impossible for law enforcement to proceed smoothly. These facilities include educated and skilled personnel, good organization, adequate equipment, and sufficient finances. The constraints related to facilities include the limited human resources of law enforcement officers.[5] The most comprehensive supporting facilities are only available at the National Police Headquarters in Jakarta, which can be a barrier when cyberporn crimes occur in other regions, such as the South Sulawesi Regional Police.[15] Community Factors, Cultural Factors

D. CONCLUSION

The process of investigating criminal acts of threats and extortion through social media with the mode of spreading immoral content in the South Sulawesi Regional Police is the same as handling other general crimes if the report is received then an investigation warrant and SP2HPA1 (Notification of the progress of the report research results) are issued. That's where investigators process the crime scene to look for information on whether the incident can be found to be a crime or not a crime., if the results of the investigation find at least 2 initial pieces of evidence that are sufficient in accordance with the provisions of Article 184 of the Criminal

Procedure Code then the status will be raised from the investigation stage to the investigation stage and the issuance of SP2HP A3 (Notification of Investigation Results) will be carried out.

E. REFERENCE

[1] M. R. H. Liviani, "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia," *UIN Sunan Ampel*, vol. 23, no. 2, 2020.

[2] M. I. Asrum, H. Thalib, and M. Jannah, "Criminological Review of the Phenomenon of Cyberbullying," *Horiz. Public Leg. Stud.*, vol. 1, no. 1, pp. 32–49, 2024, doi: 10.56087/hegels.v1i1.490.

[3] S. R. Ummah, "Pornografi Ditinjau dari Hukum Positif dan Hukum Pidana Islam," *Al-Qanun J. Pemikir. dan Pembaharuan Huk. Islam*, vol. 20, no. 1, pp. 26–35, 2018, doi: 10.15642/alqanun.2017.20.1.26-35.

[4] A. Aswari, "Perlindungan Hukum Tanpa Penegakan Hukum Dalam Sengketa Transaksi Elektronik," *Kertha Patrika*, vol. 42, no. 2, p. 163, 2020, doi: 10.24843/kp.2020.v42.i02.p05.

[5] T. S. Ramli *et al.*, "Prinsip Prinsip Cyber Law Pada Media Over the Top E-Commerce Berdasarkan Transformasi Digital Di Indonesia," *J. Legis. Indones.*, vol. 16, no. 3, pp. 392–398, 2019.

[6] Y. H. Lokapala, F. J. Nurfauzi, and Y. Widowaty, "Aspek Yuridis Kejahatan Phishing dalam Ketentuan Hukum di Indonesia," *Indones. J. Crim. Law Criminol.*, vol. 5, no. 1, pp. 19–24, 2024, doi: 10.18196/ijclc.v5i1.19853.

[7] T. Handayani, "Perlindungan Dan Penegakan Hukum Terhadap Kasus Kekerasan Seksual Pada Anak," *J. Huk. Mimb. Justitia*, vol. 2, no. 2, p. 826, 2018, doi: 10.35194/jhmj.v2i2.33.

[8] S. Yuniarti, "Perlindungan Hukum Data Pribadi Di Indonesia," *Bus. Econ. Commun. Soc. Sci. J.*, vol. 1, no. 1, pp. 147–154, 2019, doi: 10.21512/becossjournal.v1i1.6030.

[9] E. Priliasari, "PERLINDUNGAN DATA PRIBADI KONSUMEN DALAM TRANSAKSI E-COMMERCE MENURUT PERATURAN PERUNDANG-UNDANGAN DI INDONESIA (Legal Protection of Consumer Personal Data in E-

Commerce According To Laws dan Regulations in Indonesia)," *J. Rechts Vinding*, vol. 12, no. 2, pp. 261–279, 2023.

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

[11] Muhammad FauziRamadhan, M. Jannah, and A. Putera, "TERTIPU LINK , TERKURAS PRIVASI , DI MANA KEADILAN HUKUM ?," *JUDICATUM J. Dimens. Catra Huk.*, vol. 3, no. 1, pp. 236–251, 2025, doi: https://doi.org/10.35326/judicatum.v3i1.7725.

[12] M. F. Ramadhan, "Legal Review of Action Criminal Exploitation of Street Children at Crossroads in the Name of Beggars," vol. 1, no. 2, pp. 1–7, 2025.

[13] M. Fauzi Ramadhan, "Pengantar Ilmu Hukum." 2016.

[14] P. K. Nurdianto, "Jurnal Cakrawala Informasi," *Cakrawala Inf.*, vol. 1, no. 1, pp. 1–14, 2021.

[15] Sulastryani, "Peran Penyidik Dalam Penanganan Tindak Pidana Pencemaran Nama Baik Melalui Media Sosial (Studi Kasus Polres Palopo)," *J. to ciung. J. Ilmu Huk.*, vol. 1, pp. 50–63, 2021.

[16] Munadi, "Diskursus Hukum," *Sustain.*, vol. 11, no. 1, pp. 1–14, 2019, [Online]. Available: http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_SISTEM_PEMBETUNGAN_TERPUSAT_STRATEGI_MELESTARI