Law Enforcement in Dealing with the Lack of Ethics of Social Media Users by the Directorate of Cyber Crime (Dittipidsiber) Bareskrim Polri

Dedek Ervina Sitepu¹, Surya Nita², Riska Sri Handayani³

dedek_1984@yahoo.co.id¹, surya.nita@ui.ac.id², riska.sri@ui.ac.id³

¹,²,³Police Science Studies Program, School of Strategic and Global Studies, Indonesia

<table>
<thead>
<tr>
<th>Article Info</th>
<th>Abstract</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received: 2024-02-12</td>
<td>This research aims to analyze the law enforcement mechanisms carried out by the Directorate of Cyber Crime (Dittipidsiber) of the Indonesian National Police’s Criminal Investigation Department (Bareskrim Polri) in facing the lack of ethics among social media users that potentially lead to cybercrimes. With a focus on handling cybercrime cases on social media, this research reveals and analyzes the steps taken by Dittipidsiber in responding to ethical violations in cyberspace. The research methodology employed is qualitative with a case study approach. Data was collected through document studies, interviews, and observations to gain a comprehensive understanding of the law enforcement processes undertaken by Dittipidsiber. Data analysis was conducted by interpreting information obtained from these sources to construct a comprehensive understanding of the research subject. The conclusions of this research indicate that Dittipidsiber Bareskrim Polri has implemented a series of repressive and preventive efforts to address cybercrimes. These efforts include law enforcement, investigation, prosecution, infrastructure improvement, education and training, socialization and education, sanctions enforcement, as well as international cooperation. Additionally, the mechanisms for handling cybercrime cases involve both criminal and non-criminal legal policies, digital forensic analysis, and service optimization to prevent criminal activities, based on the Electronic Information and Transactions Law (UU ITE). Education and socialization to the public also play a crucial role in preventing cybercrimes.</td>
</tr>
<tr>
<td>Revised: 2024-02-21</td>
<td></td>
</tr>
<tr>
<td>Accepted: 2024-03-24</td>
<td></td>
</tr>
</tbody>
</table>

Keywords: User Ethics; Social Media; Cybercrime
I. Introduction

The influence of time and the rapid advancement of technology have had a significant impact on sociocultural changes (Meidiyanto, 2015), including the occurrence of crime. Crime has always been a persistent issue in human life, as it evolves alongside the progress of human civilization. From a sociological standpoint, crime is a social phenomenon that is connected to individuals and society. There are various paradigms that aim to explain the existence of crime. In criminology, Mubarok defines crime as a behavioral pattern that causes harm to society, resulting in a social reaction from the community (Mubarok, 2017).

The government is facing a challenging task in countering criminal techniques carried out through computer technology, particularly on internet and intranet networks (Ketaren, 2016). The rise of cybercrime poses a threat to stability, making it difficult for authorities to combat this issue. The fast growth of information technology has resulted in both good and bad outcomes, just like two sides of a coin that are connected and cannot be separated (Ketaren, 2016). Cybercrime is a product of the active utilization and increasing concentration of community life in cyberspace. As society progresses, the social and criminal burdens become increasingly burdensome, impacting the community's social life and giving rise to various forms of crime.

Cybercrime can occur intentionally or unintentionally, stemming from either ignorance or a lack of understanding about cyber ethics. Therefore, the significance of cyber ethics in the virtual realm is pivotal, given that the internet has cultivated its own interconnected community within human life. Traditional forms of communication, once reliant on postal services, have transformed into a digital landscape where letters can be composed by merely sitting in front of a computer. The imperative for ethical behavior in the virtual world is underscored by several factors: the diverse origins of internet users with distinct cultures, languages, and customs; the anonymous nature of individuals in the online sphere, allowing interactions without the need for real identity disclosure; the availability of various online facilities that empower individuals to act ethically; and the continuous growth of internet users, resulting in a constant influx of newcomers into the virtual world.

Violations of cyber ethics can lead to cyber crimes such as hacking social media accounts, creating fake news, engaging in hate speech, online fraud, and more. For example, based on the year-end records of the Jakarta Metropolitan Police, the total number of crimes handled by the Criminal Investigation Unit (Ditreskrim) of the Jakarta Metropolitan Police was 1,042 cases. This figure experienced a decrease compared to 2019, which had 1,100 cases. The cases
handled by Ditreskrimsus of the Jakarta Metropolitan Police decreased from 1,100 cases in 2019 to 1,042 cases in 2020. Out of the total number of cases, the Jakarta Metropolitan Police resolved 711 cases in 2020, while the resolution of cybercrime cases in 2019 reached 710 cases. The rate of case resolution in 2020 increased by 3 percent compared to 2019. Some cybercrime cases that drew public attention were uncovered by the Jakarta Metropolitan Police. One such case involved a TikTok user, Ratu Wiraksini (53), who referred to the police as 'dajal' (devil) for arresting Habib Rizieq Shihab. She was arrested on Monday (14/12) due to her video post accusing the police of being 'dajal' on her TikTok account @yudinratu (detik.com, December 24, 2020).

In comparison to the corresponding period in 2021, there was a significant rise in cybercrime incidents in 2022. The number of reported cybercrime cases increased by a staggering 14 times. According to data from the e-MP Robinopsnal of the Indonesian National Police’s Criminal Investigation Department (Bareskrim Polri), a total of 8,831 cybercrime cases were addressed by the police between January 1 and December 22, 2022. Both Bareskrim Polri and Regional Police (Polda) units across Indonesia actively participated in the enforcement of these cases. Among them, the Jakarta Metropolitan Police (Polda Metro Jaya) stood out with the highest number of enforcement actions, handling a total of 3,709 cases. In contrast, during the same period in 2021, there were only 612 enforcement actions carried out across Indonesia, involving a mere 26 units (Pusiknas.Polri.go.id, 2022).

In relation to the data concerning cybercrime from 2021 to 2022 within the Indonesian National Police units, particularly the Regional Police (Polda) across Indonesia, the Indonesian National Police's Criminal Investigation Department (Bareskrim Polri) also handles certain cases. Dealing with cybercrime is undeniably a challenging task, and its management differs from that of other criminal cases. Due to this, the Indonesian National Police (Polri) is continuously working on establishing a Directorate of Cyber Crime in each regional police force throughout Indonesia. The establishment of such a structure is typically determined by various factors, including the type of Regional Police (Polda), workload index, geographical conditions, resource availability, and other considerations. However, in terms of cybercrime, the Indonesian National Police is currently developing a structure to address cybercrime in different regions (Dalimunthe et al., 2022). Polri is proposing the creation of a directorate specifically dedicated to handling cybercrime at the Regional Police level. This proposal aims to enhance the expertise of investigators in dealing with cybercrimes that occur across multiple regions. This is necessary as the current enforcement efforts are still at the sub-directorate level under special criminal enforcement.
Lately, there has been a significant increase in cybercrime in Indonesia, causing substantial losses to individuals and the general public. In response to this, the Directorate of Cyber Crime (Dittipidsiber) within the Indonesian National Police’s Criminal Investigation Department (Bareskrim Polri) has been assigned the task of enforcing the law against cybercrimes. The Directorate deals with two groups of cyber-related crimes, namely computer crime and computer-related crime.

The author’s interest arises from the need to delve into the challenges posed by the lack of ethics among social media users, and the law enforcement strategies implemented by the Directorate of Cyber Crime (Dittipidsiber) in the Indonesian National Police’s Criminal Investigation Department (Bareskrim Polri). The chosen research topic holds high significance as it emphasizes the need for effective handling of ethical violations in the realm of social media, especially with the approaching 2024 General Elections that are vulnerable to such criminal actions. The aim is to maintain order and ensure public safety, with a specific focus on ethical considerations related to the use of social media. This research aims to provide valuable insights into the law enforcement strategies implemented to address unethical behavior in the world of social media, highlighting its significance in maintaining a safe and lawful environment amidst the widespread use of electronic media, social platforms, and other internet-based channels.

The main concern in this research is the effectiveness of the Indonesian National Police (Polri) in combating cybercrime. Specifically, the Directorate of Cyber Crime (Dittipidsiber) within the Criminal Investigation Department (Bareskrim Polri) plays a crucial role in protecting the public from the dangers of the virtual world. However, it is important to examine whether there are any shortcomings in terms of investigator competencies, investigative processes, and inquiry infrastructure when it comes to enforcing cybercrime laws. This research aims to uncover and analyze the mechanisms employed by Dittipidsiber in handling cybercrime cases on social media that involve ethical violations. Furthermore, it seeks to identify and analyze the repressive efforts made by Dittipidsiber Bareskrim Polri to address the lack of ethics among social media users.

2. Research Method

The research conducted in this study is qualitative and leans towards a descriptive analysis. Qualitative research emphasizes the process and meaning, with theoretical foundations guiding the focus on field-based facts. The author made general or rough observations of law enforcement practices regarding cybercrime cases through social media due to the lack of user cyber ethics, specifically within the jurisdiction of the Jakarta Metropolitan Police (Polda Metro Jaya). The study focuses on this area and will be examined repeatedly, with the
author choosing a specific focus based on the research problem.

The author employed a case study research design, a type of research widely used in social sciences. This type of research is intensive, detailed, and comprehensive, often focusing on individuals, social units (groups, families, etc.), or specific events within a certain timeframe (historical approach). The typical research questions in this type of study often start with “why.” The choice of a case study design is motivated by the author’s affiliation with the Indonesian National Police’s Criminal Investigation Department (Bareskrim Polri), providing insight into the law enforcement phenomena in response to the lack of user ethics on social media.

Data collection involves key informants or research subjects from various sources, including internal sources within Dittipidsiber Bareskrim Polri, external stakeholders, and the general public. The author employed triangulation as a data collection technique, combining various data collection methods and sources to obtain a comprehensive view of the researched phenomenon. Document study, interviews, and observations were utilized, each producing different evidence or data, contributing to diverse perspectives on the studied phenomenon. The combination of these perspectives widens the knowledge spectrum and contributes to the pursuit of truth.

The primary data sources include the opinions of individuals, consisting of leadership, task force implementers, and members of the community, as well as events related to law enforcement against cyber violations. Secondary data sources involve document and archive studies, such as reports on law enforcement activities addressing the lack of user ethics on social media. Data collection techniques include document study, interviews, and observations. Qualitative data analysis, following Miles and Huberman’s framework, involves data reduction, data presentation, and drawing conclusions or verification.

3. Results and Discussion

Mechanisms for Handling Cybercrime Cases on Social Media Involving Ethical Violations by Dittipidsiber Bareskrim Polri

The Mechanism for Handling Cybercrime Cases on Social Media Involving Ethical Violations by Dittipidsiber Bareskrim Polri involves criminal and non-criminal legal policies as well as digital forensic analysis. In Indonesia, Law Number 19 of 2016 concerning Electronic Information and Transactions (UU ITE) regulates the use of information technology and social media to uphold justice, public order, and legal certainty (Bu’ulolo et al., 2023).

The interpretation of norms contained in Article 27 paragraph (3) of the ITE Law
regarding defamation and/or defamation of character cannot be separated from criminal legal norms in Articles 310 and 311 of the Criminal Code (KUHP). Likewise, cyberbullying directed at individuals and not disseminated through media accessible to the public can be subject to legal consequences due to meeting the element of being "in public." Addressing the use of Article 27 paragraph (3) of the ITE Law can implicate any cyberbullying perpetrators wherever they may be.

Based on the explanation above, Constitutional Court Decision Number 50/PUU-VI/2008 states the following: first, declares that the petitioner does not have legal standing; second, rejects the petitioner’s entire request or at least declares the request for review cannot be accepted (niet ontvankelijk verklaard); third, accepts the government's statement in its entirety; fourth, declares that the provisions of Article 27 paragraph (3) of the ITE Law do not conflict with the provisions of Article 1 paragraph (2) and paragraph (3), Article 27 (1), Article 28, 28A; Article 28C paragraph (1) and paragraph (2); Article 28D paragraph (1), Article 28E paragraph (2) and paragraph (3); Article 28F, Article 28G paragraph (1) of the 1945 Constitution.

There is a clear and definite legal certainty in the application of Article 27 paragraph (3) of Law Number 11 of 2008 as amended by Law Number 19 of 2016 concerning Electronic Information and Transactions regarding Cyberbullying in depth. Regarding the difference from Article 310 of the Criminal Code, this crime is committed through media, not in the real world.

Legal certainty regarding the settlement of Cyberbullying cases is explicitly regulated in Article 27 paragraph (3) of Law Number 11 of 2008 as amended by Law Number 19 of 2016 concerning Electronic Information and Transactions. Moreover, considering such views have become jurisprudence, as stated in the considerations of Constitutional Court Decision Number 50/PUU-VI/2008, it has provided legal certainty for provisions regulating Cyberbullying criminal offenses.

In order to establish legal certainty, Indonesia has the Republic of Indonesia Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE), which serves as the legal framework in Indonesia for the first time in the field of Information Technology and Electronic Transactions. Subsequent changes were made with the enactment of Republic of Indonesia Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. False news is regulated in Article 28:

(1) Any person intentionally and without authority disseminating false and misleading news that results in consumer losses in Electronic Transactions.
(2) Any person intentionally and without authority spreading information aimed at creating hatred or hostility among individuals and/or specific groups in society based on ethnicity, religion, race, and inter-group relations (SARA).

The ITE Law establishes a legal framework to protect the public from illegal content and the misuse of information technology. For instance, the ITE Law regulates the dissemination of information that violates decency, gambling, defamation or character assassination, extortion, threats, spreading false news, and hatred or hostility based on ethnicity, religion, race, and group affiliations.

In the context of law enforcement, the ITE Law grants investigators the authority to conduct searches and seizures, taking into account the protection of privacy, confidentiality, smooth public services, and data integrity. Investigators are also empowered to collaborate with investigators from other countries in sharing information and evidence to uncover cybercrime.

The amendments brought by the ITE Law also emphasize the government’s role in preventing the dissemination of illegal content by taking actions to disconnect access to electronic information that violates the law. Additionally, the ITE Law acknowledges that crimes of defamation and character assassination in the field of electronic information and transactions are complaint-driven, meaning legal actions can only be taken based on complaints from the aggrieved party.

Cases such as online prostitution and defamation on social media are addressed through digital forensic analysis to gather digital evidence that can be used in prosecution (Pratamaa et al., 2022; Tamrin et al., 2022). Additionally, in handling sexting cases among adolescents, service optimization and case management are necessary to prevent such criminal acts (Cahyati et al., 2022). A study by Tamrin et al. (2022) also highlights the role of forensic linguistics in addressing cases of defamation and character assassination on social media, where language experts are involved in uncovering the meaning of language through forensic linguistic studies. Thus, handling cybercrime cases on social media involves various aspects, including criminal law, digital forensic analysis, and service optimization to prevent such criminal acts.

The motive behind Cyberbullying is different from conventional bullying where the perpetrator bullies due to a lack of attention, a tendency towards hostility, and the victimization as the underlying motives for cyberbullying actions (Pandie & Weismann, 2016). Firstly, there’s the motive of "The Vengeful Angel." In this culturally conflicted climate, numerous social groups cannot be reconciled and always find themselves in tension, competition, and social conflicts colored by feelings of hatred and vengeance.
Social media plays a crucial role in the commission of cyberbullying crimes, as it can only be carried out on platforms that rely on internet connections. Cyberbullying differs from traditional bullying, which includes physical, verbal, and mental bullying that can occur directly and conventionally. Cyberbullying, on the other hand, takes place in the virtual world, requiring networks and internet connections to commit such crimes. Secondly, social media enables online users to engage in cyberbullying due to the ease of posting and disseminating online content, as well as reacting to that content. Thirdly, the issue of cyberbullying arises with the advent of social media, as before its introduction, cyberbullying did not exist. Fourthly, Cyberbullying occurs when social media platforms such as Facebook and Twitter provide text storage facilities. Fifthly, Cyberbullying on social media has negative consequences as cases are brought to the public eye, making the available evidence easily accessible. Lastly, everyone is interconnected through social media, facilitating rapid information dissemination.

The mechanism for handling cybercrime cases on social media by the Directorate of Cyber Crime (Dittipidsiber) of the Indonesian National Police (Bareskrim Polri) involves a series of processes covering several stages, starting from early detection to prevention. Early detection is a crucial step in facing cybercrime threats, and Dittipidsiber employs advanced technology to monitor suspicious online activities. The use of cybersecurity software and big data analytics forms the foundation for early detection to identify potential ethical violations on social media.

In the detection process, Dittipidsiber also utilizes a trained team of experts to analyze suspicious online behavioral patterns. This team has a deep understanding of tactics used by cybercriminals, enabling them to more effectively monitor and detect threats. Involvement in international networks is also a crucial aspect in dealing with cybercrime cases involving global social media.

After the initial detection, the next step is the investigation phase. Dittipidsiber forms a skilled investigative team to gather strong electronic evidence. Additionally, collaboration with social media service providers is necessary to obtain further information about the ethical violations that occurred. At this stage, expertise in digital forensics becomes essential in unraveling the digital traces of perpetrators and ensuring the validity of the evidence produced.

The investigation process also involves close collaboration with other law enforcement agencies, such as the Public Prosecutor’s Office and the Court, to ensure that legal proceedings are conducted in accordance with applicable laws. The preparation of a strong indictment is a primary focus to ensure that...
cybercrime perpetrators can be thoroughly prosecuted. Dittipidsiber is committed to bringing justice to the virtual world as it applies in the real world.

The next step is the legal handling involving the trial process. In court, Dittipidsiber seeks to prove the guilt of the perpetrators using evidence collected during the investigation stage. Involvement of prosecutors in this process is crucial to ensure that the indictment prepared by Dittipidsiber meets applicable legal standards. A fair and transparent trial is expected to serve as a deterrent to cybercrime perpetrators and provide justice to the victims affected.

In addition to legal handling, Dittipidsiber also focuses on restoration and rehabilitation efforts for cybercrime victims. Victims often experience significant psychological and social impacts; therefore, restoration programs that empower victims are a crucial part of the case handling mechanism. Dittipidsiber strives to provide psychological, legal, and technical support to victims for their comprehensive recovery.

Preventive efforts are the mainstay in Dittipidsiber's mechanism for handling cybercrime cases. In addition to reactive measures after incidents, Dittipidsiber actively engages in educating and raising awareness in the community. This educational program involves various stakeholders such as schools, higher education institutions, and the general public. Education covers the use of strong passwords, understanding the risks of sharing personal information, and identifying potential signs of cyber attacks.

Dittipidsiber also conducts socialization on internet ethics, teaching safe and responsible behavior in the virtual world. Collaboration with the private sector, government institutions, and community organizations is key to creating a safer and protected cyber ecosystem. By providing better understanding to the public, Dittipidsiber hopes to reduce potential victims and hinder the growth of cybercrime activities on social media.

The importance of social media in everyday life demands that Dittipidsiber continuously develop expertise and technology in handling cybercrime cases. Strengthening capacity and enhancing cybersecurity technology are priorities to ensure effectiveness in responding to the development of new trends and tactics used by cybercriminals.

Moreover, international cooperation in handling cybercrime is also necessary. Dittipidsiber continues to build relationships and collaborate with international cyber institutions for information exchange and coordination in addressing global cyber threats. Thus, Dittipidsiber not only focuses on cases involving national social media but also takes a global perspective in efforts to suppress cybercrime activities.
The sustainability of the cybercrime case handling mechanism is also supported by the implementation of relevant laws and regulations. Dittipidsiber continues to monitor legal developments related to cybercrime and contributes to the formulation of policies that can strengthen law enforcement in this field. Clear and firm regulations provide the foundation for a strong legal basis in taking action against cybercrime perpetrators.

Repressive Efforts in Addressing the Lack of Ethics Among Social Media Users by Dittipidsiber Bareskrim Polri

Repressive measures can take the form of (1) the police taking action by visiting the crime scene (TKP) to apprehend and detain cybercrime suspects, leading to subsequent processing and trial according to the severity of the committed offense, and (2) employing restorative justice as a resolution approach for the victims (Syam, 2015). In conducting a police investigation into cyberbullying crimes, the primary objectives of the investigation must be determined at the earliest stage, along with the following provisions: a) Confirm whether the violation has occurred or not; b) Collect all available information, materials, intelligence, and evidence; c) Act in the interest of justice; d) Strictly adhere to all reasonable inquiries; e) Conduct a thorough investigation; f) Identify, apprehend, and prosecute the violators; and g) Present all evidence to the prosecutor (Akhgar & Staniforth, 2011).

In Indonesia, legal regulations related to cyberbullying offenses still refer to Law Number 2 of 2008 concerning Information Technology and Electronic Transactions, particularly in Article 27 paragraphs (1), (2), (4), and Article 29. These articles prohibit the distribution and transmission of electronic information and/or electronic documents containing acts of obscenity, defamation, character assassination, and threats (Sanda, 2016). Articles that can be used to prosecute Cyber Bullying perpetrators are Articles 310 and 311 of the Criminal Code (KUHP) and Article 27 paragraph (3) of the ITE Law regarding defamation. Criminal acts of defamation in the Criminal Code are regulated as a complaint offense, where there must be a complaint from the victim who feels that their good name has been tarnished for the perpetrator to be charged under these articles (Sanda, 2016). Perpetrators who violate Article 27 paragraph (3) of the Information Technology and Electronic Transactions Law and KUHP Articles 310 and 311 are punished with imprisonment for up to 6 (six) years and/or a fine of up to IDR 1,000,000,000.00 (one billion rupiahs) (Indonesia, 2008); (Ekaputra & Kahir, 2010). Additionally, the resolution of cyberbullying cases falls under the majority category of "Delik Aduan" (complaint offense), with two subcategories: relative complaint offenses and absolute complaint offenses. Relative complaint
offenses only qualify as complaint offenses under certain circumstances, such as Article 367 paragraphs (1), (2), and (3) of the Criminal Code, as well as Article 370, Article 376, and Article 394 of the Criminal Code. Absolute complaint offenses are offenses that always qualify as complaint offenses regardless of the circumstances, such as defamation (Articles 310-319 of the Criminal Code), Article 284, 287, 293, and 332 of the Criminal Code. The identification of cases categorized as complaint offenses and the decision to proceed with the trial are determined primarily by the victim or their family. The victim can also halt the proceedings if there is an agreement between the victim and the perpetrator regarding the compensation that the perpetrator must pay (Raharjo, 2008).

One form of effort to raise awareness about the dangers of the online world is when the community service lecturer presents several slides containing information about individuals ranging from suspects to convicts of violations of the ITE Law. Hence, the information shared gives a general idea to everyone that as long as we browse the internet, there are numerous articles in the ITE Law that are hiding. Law Number 19 of 2016 concerning Electronic Information and Transactions or the ITE Law still ensnared several individuals throughout the year 2020.

Repressive efforts are conceptual crime prevention measures taken after the crime has occurred. Repressive measures are intended to take action against criminals according to their deeds and rectify them so that they realize that their actions violate the law and harm society. This is done to prevent them from repeating such actions, and others will refrain from doing so considering the severe sanctions they will face.

Repressive efforts are related to law enforcement that results in penalties that can have a deterrent effect on the perpetrators. The lack of police understanding of technology has led to some challenges in the investigation process. Inadequate facilities and infrastructure to support police performance, a limited number of personnel, and a cultural shift over time eroded by modernization, demanding practicality, are inhibiting factors in the law enforcement carried out by Dittipidsiber Bareskrim Polri.

Repressive efforts in addressing the lack of ethics among social media users by Dittipidsiber Bareskrim Polri involve legal enforcement measures taken after a violation or cybercrime has occurred. These efforts are part of the legal system, which includes the structure, substance, and legal culture. The structure is likened to the engine that operates the law, substance is what the engine does and produces, and legal culture determines how the engine is used.

In the context of law enforcement against cybercrime, repressive efforts become the last resort used after non-penal efforts such as preventive and preemptive...
measures. Repressive efforts involve resolving and combating crimes on social media through criminal law. This means that Dittipdisiber Bareskrim Polri will conduct investigations, prosecutions, and legal processing against individuals or groups proven to have committed cybercrimes due to the lack of ethical use of social media.

Repressive efforts in addressing the lack of ethics among social media users by Dittipdisiber Bareskrim Polri include legal actions against committed violations. This may involve investigations, enforcement, and legal action against content that violates the law on social media. Additionally, repressive efforts may also include the socialization of legal rules related to social media use to increase awareness of ethics in social media behavior.

Repressive efforts in addressing the lack of ethics among social media users involve law enforcement measures taken after a violation or crime has occurred. Here are several repressive steps that can be taken:

1. **Law Enforcement**: Taking legal action against individuals who violate the rules or legal norms on social media, such as spreading fake news, hate speech, or online harassment.
2. **Investigation and Prosecution**: Conducting investigations and prosecuting cybercrime, including document forgery or online fraud, using existing legal regulations.
3. **Infrastructure Improvement**: Enhancing adequate infrastructure to maximize the performance of law enforcement in investigating and combating cybercrimes.
4. **Education and Training**: Providing training related to technology and information, particularly in the cyber field, to law enforcement officials to enhance the quality and quantity of personnel dealing with cybercrimes.
5. **Socialization and Education**: Organizing socialization in collaboration with relevant parties, such as the Ministry of Health, Indonesian Medical Association, and the Ministry of Communication and Informatics, to educate the public about the negative impacts of unethical behavior on social media.
6. **Implementation of Sanctions**: Imposing severe sanctions on cybercriminals to create a deterrent effect, preventing perpetrators and others from repeating or engaging in similar actions.
7. **International Cooperation**: Given the global nature of social media, international cooperation is necessary to address cross-border cybercrimes. This involves coordination with international law enforcement agencies and organizations such as Interpol to facilitate extradition, information exchange, and enforcement against cybercriminals.
Societal awareness of legal regulations and law enforcement is a crucial step in addressing the lack of ethics among social media users. Additionally, preventive approaches such as education and advocacy need to be enhanced to improve public understanding of the ethics of using social media.

Moreover, repressive efforts can also involve collaboration with relevant parties, such as social media service providers, to identify and take action against cybercriminals. This is done by leveraging the definitions and concepts of social media that enable the creation and exchange of content by users, which may include content that violates the law.

In practice, repressive efforts must always be balanced with a profound understanding of cyber ethics and cybersecurity awareness among social media users to ensure effective law enforcement without compromising legitimate freedom of expression.

4. Conclusion

The mechanism for handling cybercrime cases on social media involving ethical violations by the Directorate of Cyber Crime (Dittipidsiber) within the Indonesian National Police (Bareskrim Polri) encompasses several strategic steps. Firstly, Dittipidsiber utilizes advanced technology for early detection of suspicious online activities, including the use of cybersecurity software and big data analytics. Trained expert teams are deployed to analyze online behavioral patterns and identify potential ethical violations on social media. Furthermore, the case handling mechanism involves both criminal and non-criminal legal policies along with digital forensic analysis. The Electronic Information and Transactions Law (UU ITE) provide a robust legal basis for addressing cybercrime, with legal norms related to defamation and slander.

In repressive efforts, Dittipidsiber can take direct actions such as visiting the crime scene (TKP) for the arrest and detention of suspects. Additionally, there are resolution steps through restorative justice for the victims. The police investigation process into cyberbullying crimes must determine the main objectives of the investigation, collect evidence, and act in the interest of justice. Dittipidsiber also monitors legal developments related to cybercrime and contributes to the formulation of policies that strengthen law enforcement in this field. International cooperation is also a crucial aspect in addressing cybercrime cases involving global social media platforms.
References


