

## Qualitative Criminological Analysis Of The Influence Of Social Media On Cybercrime Patterns Of Adolescents

Radityo Wirananto<sup>1)</sup>, Aghastyar<sup>2)</sup>, Young Allan Loway<sup>3)</sup>, Pietro Grassio Ekoyulio<sup>4)</sup>,  
<sup>1,2,3,4)\*</sup> Pelita Harapan University

\*Corresponding Author

Email: [01051230184radityowirananto@gmail.com](mailto:01051230184radityowirananto@gmail.com), [01051230170aghastyar03@gmail.com](mailto:01051230170aghastyar03@gmail.com),  
[01051230104vanolowayvy@gmail.com](mailto:01051230104vanolowayvy@gmail.com), [pietro.ekoyulio@lecturer.uph.edu](mailto:pietro.ekoyulio@lecturer.uph.edu)\*

---

### Abstract

*The rapid development of social media has transformed patterns of social interaction among urban youth while simultaneously creating new opportunities for cybercrime. Social media functions not only as a communication platform but also as a digital environment where values, behaviors, and social identities are constructed. This study aims to analyze the influence of social media on cybercrime patterns among urban Indonesian youth through a qualitative criminological approach. The research employs a qualitative method with descriptive-analytical specifications using a literature-based approach. Data were collected from academic journals, books, research reports, and relevant legal documents and analyzed through qualitative content analysis. The findings reveal that social media significantly contributes to the emergence of cybercrime patterns among urban youth, particularly in the forms of cyberbullying, hate speech, online fraud using fake accounts, dissemination of personal data, and basic hacking activities. The study also identifies three major criminogenic factors underlying cybercrime involvement: individual factors, including low digital literacy, weak self-control, and the need for social recognition; social factors, including limited parental supervision, inadequate digital education, and strong peer-group influence; and structural factors, including widespread internet access, weak perceptions of law enforcement effectiveness, and the anonymity provided by digital platforms. Furthermore, the findings indicate that many young people engage in cybercrime not primarily for economic gain but due to curiosity, experimentation, online popularity, and peer pressure. Social media also facilitates the formation of online subcultures that normalize and reinforce deviant behavior through continuous interaction and social validation. This study concludes that cybercrime among urban Indonesian youth is a multidimensional phenomenon resulting from the interaction of individual, social, and structural factors within digital environments. Therefore, effective prevention requires integrated strategies involving digital literacy enhancement, family and school-based social control, ethical digital education, and adaptive cybercrime policies that respond to technological developments.*

**Keywords:** *Cybercrime; Qualitative Criminology; Social Media*

---

## INTRODUCTION

The development of digital technology has transformed the way teenagers interact, build relationships, and express themselves. Social media has become a primary platform for young people to communicate, seek recognition, and even establish their identities. In Indonesia's major cities, fast internet access and near-ubiquitous smartphone ownership mean that teenagers are growing up in a highly connected online environment. This situation brings significant benefits, such as ease of accessing information and expanding networks friendship. However, on the other hand, the digital space also opens up opportunities for various forms of cybercrime. The phenomenon of cybercrime among urban youth can no longer be viewed as an isolated incident. Cyberbullying, unauthorized distribution of intimate content, online fraud, and even hacking of social media accounts are becoming increasingly common. This increase is inextricably linked to the high intensity of digital platform use. Ananta, Ambodo, and Tohawi (2024) noted that the growth of social media users in Indonesia goes hand in hand with the rise in cybercrime cases. Lack of digital literacy increases the risk of technology misuse. Teenagers who lack mature self-control are a vulnerable group, both as victims and perpetrators.

Dakota and Valensia's (2025) study showed that exposure to negative content and unlimited interaction on social media can influence deviant behavior. Teenagers often imitate actions they see online. What goes viral is considered normal. The line between jokes and violations of the law becomes blurred. Chatlina and Kuswandi (2025) even emphasized that social media plays a role in shaping criminal behavior through the social learning process. Teenagers absorb values and behavioral patterns from their digital environment. When deviant behavior gains attention and popularity, the tendency to imitate it increases. A criminological perspective helps explain this phenomenon more deeply. Situmeang (2021) explains that differential association theory states that criminal behavior is learned through social interactions. These interactions are no longer limited to physical spaces. The online environment has become a new arena where values and norms are exchanged. Social control theory is also relevant. Weak family and school supervision of digital activities allows adolescents to explore cyberspace more freely without clear boundaries. Opportunities to commit crimes increase when the risk of being caught is perceived as low.

Adorjan and Ricciardelli (2018) describe the lives of modern adolescents as part of a digital ecosystem rife with surveillance practices, data tracking, and public exposure. The concept of cyber-risk explains how risks in cyberspace arise from a combination of technology, user behavior, and social structures. Adolescents are not only victims of digital risks but can also become perpetrators of crimes, tempted by anonymity and easy access. A disguised identity provides a false sense of security. As a result, actions that would not be carried out in the real world become easier to commit online. Research by Hukom and Setiadi (2025) using a netnographic approach shows that crime patterns in the digital era evolve according to the dynamics of online communities. Closed groups and anonymous forums can serve as platforms for sharing strategies for committing crimes. Solidarity is formed among perpetrators through regular interactions in digital spaces. This pattern demonstrates that social media is not simply a tool, but rather a social environment that shapes a specific culture. Davidson and Farr (2026) explain that adolescent involvement in cybercrime has complex pathways of entry and exit. Individual factors such as curiosity and the need for recognition interact with environmental factors such as online social interactions. Some adolescents become involved out of a sense of experimentation, while others are driven by peer pressure. Breaking out of this cycle requires social support and appropriate rehabilitative approaches.

The emerging issues are not solely related to the high rate of cybercrime. A more fundamental question is how social media influences the formation of crime patterns among urban Indonesian youth. How do they interpret actions taken in digital spaces? Are they aware of the legal consequences? How do online interactions shape perceptions of right and wrong? These questions require a qualitative approach to explore subjective experiences in depth. A review of previous research shows a tendency to use quantitative methods to measure the relationship between social media usage intensity and crime rates. Statistical data is important, but it does not fully explain the social dynamics underlying these actions. Syahrir (2025) highlights the effectiveness of punishment for cybercrime perpetrators, but focuses more on law enforcement aspects. Yanto and Salim (2025) discuss the influence of social media on public perceptions of crime and law enforcement. There is still room for a deeper understanding of adolescents' experiences as actors in the digital ecosystem.

The gap between *das sollen* and *das sein* is evident in this context. Normatively, social media is expected to be a means of education, creativity, and positive participation for the younger generation. Legal regulations already address child protection in the digital space and sanctions for perpetrators of cybercrime. Ideally, the online environment should be a safe and productive space. The reality on the ground shows otherwise. Misuse of digital platforms continues. Digital literacy is not yet evenly distributed. Supervision by families and educational

institutions often lags behind the pace of technological development. Normative expectations have not been fully met in practice. The development of a networked society has changed patterns of social interaction and opened up new opportunities for deviant behavior in the digital space (Ramadani, 2025). Digital media creates new opportunities for crime due to weak social control in cyberspace and the anonymity of internet users. Peer interactions on social media play a significant role in the learning process of deviant behavior, including digital fraud, hacking, and cyberbullying in adolescents (Nurmasitah et al., 2025). Cybercrime is growing as the younger generation's dependence on digital technology increases and cybersecurity literacy declines (Ananta et al., 2024). This study focuses its analysis on the local Indonesian context using a qualitative approach that emphasizes social meanings and interpretations. A qualitative criminological approach allows researchers to understand how adolescents interpret their actions, how social pressures operate within online communities, and how values and norms are formed through digital interactions. This research goes beyond measuring the frequency of violations to exploring the social processes underlying them. This perspective is expected to provide a conceptual contribution to the development of digital criminology studies in Indonesia. The purpose of this study is to analyze in-depth the influence of social media on cybercrime patterns among urban Indonesian youth through a qualitative criminological approach. This research also aims to identify criminogenic factors that emerge in online interactions and formulate implications for prevention policies and digital literacy education. The study's findings are expected to form the basis for developing more adaptive strategies to address the dynamics of cybercrime among the younger generation.

## RESEARCH METHODS

This research is a qualitative study with descriptive-analytical specifications that aims to examine in depth the influence of social media on cybercrime patterns among urban Indonesian youth through conceptual and empirical analysis. According to Waruwu (2024), qualitative research is a research procedure that produces descriptive data in the form of written or spoken words and observable behavior from the subjects studied. This approach is used to understand social phenomena holistically from the participants' perspectives within their natural settings. The method used is library research, which is research in which all data is obtained from written sources without field data collection. The approach applied is a qualitative criminology approach, with an emphasis on the analysis of criminological theories, cyber-risk concepts, and social dynamics in the digital space related to adolescent deviant behavior. Data collection techniques were carried out through documentary studies of national and international scientific journals from the last five years, criminology reference books, research reports, and regulations relevant to cybercrime and child protection in Indonesia. These sources were selectively selected based on their credibility, thematic relevance, and their contribution to the development of the analytical framework. The data analysis method uses content analysis techniques, namely by identifying main ideas, grouping findings based on certain themes, then interpreting the relationships between concepts to find patterns and trends. The analysis process is carried out systematically through the stages of data reduction, categorization, interpretation, and drawing conclusions. Data validity is maintained by comparing various sources (literature triangulation) to obtain a comprehensive synthesis. This approach is expected to produce a comprehensive understanding of the social construction and criminogenic factors that influence cybercrime patterns among urban youth in the context of social media.

## RESULTS AND DISCUSSION

### Results

#### 1. Cybercrime Patterns Among Urban Youth

A literature review shows that cybercrime patterns among urban Indonesian youth have experienced significant changes in terms of form, motive, and methods of implementation. Social media is no longer merely used as a communication tool, but has developed into a social space that shapes habits, lifestyles, values, and behavioral perspectives among adolescents. The rapid growth of digital technology and internet accessibility has increased adolescents' intensity of interaction in cyberspace, making online environments highly influential in shaping social behavior. Various studies indicate that the most common forms of cybercrime among adolescents include cyberbullying, hate speech, online fraud through fake accounts, dissemination of personal data, spreading false information, and simple hacking activities conducted to gain recognition or demonstrate technical skills. These forms of cybercrime are often perceived by adolescents as harmless actions because they occur in virtual environments without direct physical confrontation. Consequently, many adolescents underestimate the legal and social consequences of their online behavior.

The study by Ananta, Ambodo, and Tohawi (2024) emphasized that increased social media use is directly proportional to the opportunity for digital crime to occur. Adolescents who actively use multiple social media platforms tend to be more exposed to risky content, online conflicts, and broader social networks, thereby increasing their vulnerability to deviant behavior. Dakota and Valensia (2025) also found that unrestricted interaction in digital spaces facilitates the spread of deviant behavior through imitation mechanisms. Actions initially perceived as jokes may gradually escalate into legal violations when they involve threats, blackmail, hate speech, or disclosure of personal information. Urban adolescents also face strong social pressure related to popularity, social existence, and recognition. Social media has become a central platform for gaining validation and building social identity. Chiara Belva Chatlina (2025) revealed that criminal behavior in digital spaces is often driven by adolescents' desire to gain recognition from peer groups. Online popularity and visibility are increasingly viewed as indicators of social success, causing some adolescents to engage in risky or controversial behavior to attract attention.

Emerging cybercrime patterns also demonstrate adaptation to technological developments. Hukom and Setiadi (2025), through a netnographic approach, explained that online communities can form subcultures that tolerate or even encourage legal violations. Closed groups and anonymous forums frequently become spaces for exchanging information about digital fraud, hacking methods, and techniques for bypassing digital security systems. Group solidarity within online communities strengthens adolescents' confidence to engage in deviant behavior because such actions are normalized within the group environment. Literature analysis further shows that cybercrime among adolescents is not always motivated by financial gain. Davidson and Farr (2026) explain that involvement in cybercrime often begins with curiosity, technological experimentation, entertainment motives, or peer pressure. Over time, repeated exposure and social reinforcement can encourage adolescents to engage in more serious digital violations.

#### 2. Criminogenic Factors in Digital Space

Criminogenic factors influencing cybercrime among urban youth can be understood through individual, social, and structural dimensions. These factors interact with one another and collectively shape adolescents' vulnerability to engaging in cybercrime. Individual factors include low digital literacy, weak self-control, emotional instability, curiosity toward technology,

and the need for social recognition. Adolescents who lack emotional maturity are more easily provoked by online conflicts and harmful digital interactions. In addition, adolescents with technological skills but limited ethical awareness may misuse digital knowledge for illegal purposes.

Social factors relate to the roles of family, school, peer groups, and online communities. Parental supervision of adolescents' digital activities is often limited due to technological knowledge gaps and differences in digital adaptation between generations. Schools also have not fully integrated digital literacy and cyber ethics education comprehensively. Meanwhile, peer groups and online communities strongly influence adolescent behavior because support and validation from online groups can encourage actions that individuals may not perform in offline environments. Structural factors include widespread internet access, rapid technological development, and weak law enforcement in certain cybercrime cases. Syahrir (2025) explained that difficulties in tracing digital identities and proving cybercrime cases can create the perception that the risk of being caught is relatively low. This perception potentially encourages adolescents to commit cybercrime more freely because digital violations are viewed as difficult to detect. Public perception of cybercrime is also shaped by narratives circulating on social media. Yanto and Salim (2025) found that viral information significantly influences public attitudes toward crime and law enforcement. When laws are perceived as weak or inconsistently enforced, adolescents may gradually lose respect for legal norms in digital spaces.

### **3. Implications of Social Media on Cybercrime Prevention Among Urban Youth**

The literature analysis demonstrates that preventing cybercrime among adolescents requires comprehensive strategies involving families, schools, communities, digital platforms, and the government. Prevention cannot rely solely on punitive legal approaches because cybercrime is closely related to social interaction, identity formation, and technological adaptation. The findings indicate that strengthening digital literacy is one of the most important preventive measures. Adolescents need to understand digital ethics, legal consequences, cyber security awareness, and responsible online behavior. Digital literacy education is essential to help adolescents critically evaluate online content and understand the long-term impact of digital actions.

Families also play a crucial role through supervision, communication, and emotional support regarding adolescents' online activities. Effective parental involvement can help adolescents develop self-control and avoid harmful online environments. Educational institutions are expected to integrate digital ethics and cyber awareness more systematically into learning processes so that students understand both the benefits and risks of technology. In addition, social media platforms and online communities should encourage healthier digital environments by reducing harmful content and strengthening reporting mechanisms against cyber violations. The analysis also shows that law enforcement institutions need to improve technological capabilities and adaptive regulations to respond to rapidly developing cybercrime patterns. Collaboration between legal institutions, schools, families, and digital communities is essential to create a safer and more responsible digital ecosystem for adolescents.

### **Discussion**

The findings above can be interpreted through several criminological perspectives. From the perspective of Edwin H. Sutherland's Differential Association Theory, cybercrime behavior among adolescents develops through interactions within digital communities. Adolescents learn deviant behavior from peers, online groups, and viral content that normalize or even encourage illegal activities. The digital environment functions as a new socialization space where criminal techniques, motivations, and rationalizations are transmitted continuously.

Furthermore, the concept of cyber-risk proposed by Thomas Adorjan and Richard Ricciardelli explains that cybercrime emerges from the interaction between technology, social

structure, and individual behavior. Adolescents operate in digital environments that simultaneously provide freedom, anonymity, and weak social supervision. This condition creates an illusion of security, encouraging adolescents to engage in risky behavior because they believe their identities cannot easily be traced. The findings also reflect the relevance of social control theory. Weak parental supervision, limited digital literacy education, and inadequate social monitoring reduce adolescents' attachment to conventional norms. In digital spaces, adolescents may feel detached from direct social consequences because interactions occur virtually. As a result, moral restraint becomes weaker, especially when online communities provide support or validation for deviant behavior. From a structural perspective, the persistence of cybercrime among urban youth also indicates a gap between legal norms and social reality. Although regulations concerning cybercrime and child protection already exist, enforcement remains inconsistent and technological adaptation is often slower than the development of digital platforms. This condition reinforces adolescents' perceptions that cybercrime carries relatively low risk compared to conventional crimes. Overall, the findings confirm that cybercrime among urban Indonesian youth is a multidimensional phenomenon influenced by individual vulnerability, peer interaction, technological opportunity, and structural weaknesses in social control. Therefore, prevention strategies cannot rely exclusively on punitive legal approaches. More effective solutions require strengthening digital literacy, improving family and school supervision, developing ethical awareness in digital spaces, and creating policies that are adaptive to technological developments and youth social dynamics.

## CONCLUSION

The conclusion of this study indicates that social media has a significant influence on the formation of cybercrime patterns among urban Indonesian youth. Digital space not only serves as a means of communication and self-expression, but also serves as a social environment that shapes the values, perceptions, and behaviors of the younger generation. The high intensity of social media use, the need for social recognition, and the ease of access and anonymity create opportunities for various forms of deviance, such as cyberbullying, online fraud, and misuse of personal data. The emerging crime patterns are the result of a complex interaction between individual, social, and structural factors, where weak digital literacy, lack of supervision, and low perception of legal risk reinforce the tendency to commit violations. The gap between the normative expectation that social media should be an educational space and the reality of increasing cybercrime demonstrates the need for a more comprehensive approach. Qualitative criminological analysis provides insight that adolescent involvement in cybercrime is not always driven by economic motives, but often stems from social learning processes, peer pressure, and the search for identity. Therefore, prevention efforts cannot simply rely on law enforcement but need to be accompanied by strengthening digital literacy, establishing adaptive social control, and collaboration between families, schools, and the government in creating a safer digital ecosystem. This integrated approach is expected to reduce the potential for cybercrime while supporting the development of adolescents as responsible digital citizens.

## REFERENCES

- Adorjan, M., & Ricciardelli, R. (2019). *CYBER-RISK AND YOUTH DIGITAL CITIZENSHIP , PRIVACY , AND SURVEILLANCE* (Routledge). Routledge.
- Ananta, K. D., Ambodo, T., & Tohawi, A. (2024). Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia. *Islamic Law: Jurnal Siyazah*, 9(2), 118–131.
- Chatlina, C. B., & Kuswandi. (2025). Pengaruh Media Sosial terhadap Perilaku Kriminal Remaja di Indonesia. *Parleментар : Jurnal Studi Hukum Dan Administrasi Publik*, 2(4), 114–131.
- Dakota, A. D., & Valensia. (2025). Pengaruh Sosial Media terhadap Peningkatan Kejahatan di Kalangan Remaja di Indonesia. *Jurnal Multidisiplin Ilmu Akademik*, 2(2), 311–315.
- Davidson, julia, & Farr, R. (2026). *PATHWAYS INTO AND OUT OF YOUTH CYBERCRIME*. Routledge.
- Hukom, R., & Setiadi, M. H. (2025). Pengaruh Media Sosial terhadap Pola Kejahatan di Era Digital: Studi Kriminologi dengan Pendekatan Netnografi. *PERKARA :Jurnal Ilmu Hukum Dan Politik*, 3(1), 750–768. <https://doi.org/10.51903/perkara.v3i1.2353>
- Kartono, Yanto, O., & Salim, A. (2025). The Influence of Social Media on Public Perception of Crime and Law Enforcement. *IJLSSM : International Journal Of Law Social Sciences and Management*, 2(4).
- Nurmasitah, S., Bella, S. A., Na'am, M. F., & Musdalifah. (2025). EKSPLOKASI PERILAKU CYBERBULLYING REMAJA DI MEDIA WHATSAPP: PERAN POLAN KOMUNIKASI DALAM KELUARGA. *JKKP (Jurnal Kesejahteraan Keluarga Dan Pendidikan*, 12(1), 15–26.
- Ramadani, W., B, N. J., & S, D. A. (2025). Dampak Media Sosial terhadap Struktur Sosial : Tinjauan Sosiologi Komunikasi. *JISH : Jurnal Ilmu Sosial Dan Humaniora*, 1(3), 724–730.
- Situmeang, S. M. (2021). *BUKU AJAR KRIMINOLOGI*. Rajawali Buana Pustaka.
- Syahrir, M., & Saktiah. (2025). Efektivitas Hukuman bagi Pelaku Kejahatan Siber di Indonesia: Analisis Kriminologi dengan Metode Content Analysis. *PERKARA :Jurnal Ilmu Hukum Dan Politik*, 3(1), 694–711. <https://doi.org/10.51903/perkara.v3i1.2343>
- Waruwu, M. (2024). Pendekatan Penelitian Kualitatif : Konsep , Prosedur , Kelebihan dan Peran di Bidang Pendidikan. *Afeksi: Jurnal Penelitian Dan Evaluasi Pendidikan*, 5(2), 198–211