ADLIYA: Jurnal Hukum dan Kemanusiaan – ISSN: 1978-8312 (p), 2657-2125 (e)
Vol. 19, no. 1 (June 2025), pp. 39-56, doi: 10.15575/adliya.v19i1.40404

CYBERCRIME AND DIGITAL SOCIETY IN INDONESIA: LEGAL CHALLENGES AND PUBLIC DISCOURSE

Dedek Kusnadi[1], Ghina Nabilah Effendi[2] Dulce Martins da Silva[3]

[1]*Faculty of Syariah, Islamic University of Sulthan Thaha Saifuddin Jambi, Indonesia*
[2]*Faculty of Syariah, Islamic University of Sulthan Thaha Saifuddin Jambi, Indonesia*
[3]*International Coperation and Peacebulding Waseda University, Tokyo, Japan*

[*]*Correspondence: dedekkusnadi@uinjambi.ac.id*

Received: November 7, 2024; Accepted: June 2, 2025; Published: June 30, 2025

Abstract
Cybercrime is a communication technology offence that disrupts the public through the use of computers and the internet. It occurs due to the negative impact of technology affecting human life. Regarding legal protection, the government is obligated to protect every citizen from harmful actions, including cybercrime, which can cause both material and non-material harm to its users. Therefore, this study aimed to analyse cybercrime, which had become a global threat to both national and international security. Although cyber-related analysis had been widely conducted, studies focusing on the content analysis of cybercrime within the context of digital-era law remained limited. This study specifically examined the content of cybercrime discourse in Indonesia's digital society. A descriptive qualitative method was adopted with data sourced from big data on social media, official reports, and journalistic materials related to the topic. Data analysis was carried out using the NVivo 12 Plus software and word processing applications for qualitative analysis. The results showed that cybercrime content on social media, particularly Twitter, was predominantly harmful, with 77.62% classified as moderately negative and 22.38% as very negative. The consistent use of the hashtag showed the widespread nature of cybercrime. Furthermore, the digital legal framework in Indonesia was found to be insufficient in addressing the complexities of cybercrime, rendering law enforcement weak and hampered by various structural and technical challenges.

Keywords: cybercrime, law, digital society.

Abstract:
Cybercrime adalah kejahatan teknologi komunikasi yang meresahkan masyarakat melalui media komputer dan internet. *Cybercrime* terjadi akibat dampak negatif teknologi yang mempengaruhi kehidupan manusia. Terkait perlindungan hukum, pemerintah berke-wajiban melindungi setiap warga negara dari tindakan merugikan termasuk *cybercrime* yang merugikan material maupun non material bagi penggunanya. Penelitian bertujuan menganalisis *cybercrime* yang menjadi bencana global bagi keamanan nasional dan global. Penelitian terkait *Cyber* banyak dilakukan, tetapi penelitian analisis konten #*cybercrime* yang dikaji melalui hukum di era digital sangat minim. Penelitian ini berfokus pada konten #*cybercrime society in digital era* Indonesia. Metode yang digunakan adalah deskriptif kualitatif dan sumber data dari *big data social media*, dokumen laporan dan jurnalistik berkaitan dengan topik penelitian. Analisis data melalui aplikasi Nvivo12 plus, aplikasi pengolahan kata, berupa *qualitative* data analysis. Hasil penelitian menunjukkan bahwa #*cybercrime* di media

sosial, khususnya Twitter, mencerminkan dominasi konten negatif, dengan 77,62% tergolong negatif sedang dan 22,38% sangat negatif. Intensitas hashtag tetap tinggi dan menjadi indikator maraknya kejahatan siber. Sistem hukum digital di Indonesia dinilai belum memadai menghadapi kompleksitas *cybercrime*, sehingga penegakan hukumnya masih lemah dan menghadapi berbagai kendala struktural serta teknis.

Keywords: hukum; kejahatan dunia maya; masyarakat digital.

Introduction

The digital era, driven by mass communication media via the internet, is analogous to a coin that has two different sides. On the one hand, it can transform an inefficient world into a fast-paced, digitally based aspect. On the other hand, it poses a new threat to society, particularly through the increasing sophistication of mass communication technologies, which give rise to various new crimes known as cybercrime.[1] The development of technology also introduces multiple new mechanisms that change the social environment of the community, both in terms of mindset, social interaction, and social relations, giving birth to a new form of the press.[2] In this digital era, the latest news is disseminated through mass communication media or social media platforms, such as Facebook, Twitter, Instagram, WhatsApp, and various other channels.[3]

Social media has become a popular tool for interaction and even a necessity for people and groups in cyberspace. Its usage continues to grow in tandem with the global human population.[4] As of 2024, there are approximately 5.35 billion active internet users worldwide, accounting for about 66.2% of the global population, with an annual growth rate of nearly 2% (Data Reportal, 2024). Additionally, the number of mobile phone users has increased to approximately 5.81 billion, accounting for 70.7% of the global population, with smartphone connections reaching 7.4 billion[5] (Data Reportal, 2024). Data from[6] the number of internet users in Indonesia stands at 73.7% with an increase of 8.9%, or the

1 Saiful Bahri, "Communication Strategies in Building Public Trust Based on Cyber Public Relations," *Proceeding of International Conference on Education, Society and Humanity* 2, no. 1 (2024): 535–46, https://ejournal.unuja.ac.id/index.php/icesh/article/view/7918.

2 Lukmanul Hakim, Tien F. Kusumasari, and Muharman Lubis, "Text Mining of UU-ITE Implementation in Indonesia," *Journal of Physics: Conference Series* 1007, no. 1 (2018), https://doi.org/10.1088/1742-6596/1007/1/012038.

3 Vita Cita Emia Tarigan et al., "Cybercrime Case on Social Media in Indonesia," *International Journal of Civil Engineering and Technology* 9, no. 7 (2018): 783–88, https://iaeme.com/Home/article_id/IJCIET_09_07_081.

4 Kadek Devina Ellyona Putri, Mariano Wawan Latbin, and Gerald Aldytia Bunga, "Phenomenom Cyber Crime in Indonesia in the Digitalization Era," *Journal of Digital Law and Policy* 3, no. 2 (2024): 99–109, https://doi.org/10.58982/jdlp.v3i2.549.

5 Adi Ahmad, Riyan Maulana, and Muhammad Yassir, "Cybersecurity Challenges In The Era Of Digital Transformation A Comprehensive Analysis Of Information Systems," *Journal Informatic, Education and Management (JIEM)* 6, no. 1 (2024): 7–11, https://doi.org/10.61992/jiem.v6i1.57.

6 APJII, "Survei Pengguna Internet Indonesia" (APJII, 2020).

equivalent of 25.5 million users, bringing the total to 196.7 million users, nearly reaching 200 million out of a total population of 266.9 million. The use of social media influences behaviour and can foster indifference toward the immediate environment. Social media is considered a factor that influences moral development.[7] According to a report from http://tekno.liputan6.com, as referenced in the Akamai Report, State of the Internet Report, and Symantec Internet Security Threat Report, Indonesia ranks among the top five countries with the most significant number of social media users. It holds the sixth position globally in terms of the number of cyberattacks (38%) out of 10 countries. A study revealed that, over the past three years, Indonesia experienced 36.6 million cybercrime attacks. Some cases of cybercrime that occurred in Indonesia included the following.

First, on Saturday, April 17, 2004, a hacker named Dani Firmansyah, an Information Technology (IT) consultant at PT Danareksa in Jakarta, successfully breached the website of the National Election Tabulation Centre of Indonesia's General Elections Commission (KPU) hosted at http://tnp.kpu.go.id. Operating from Hotel Borobudur in Central Jakarta, the hacker modified the election data by changing the names of political parties to "unique" or humorous alternatives. This incident exposed the vulnerability of the government's digital infrastructure and attracted significant public and media attention to cybersecurity issues in Indonesia.[8] *Second*, a cybersex case handled by Polda Metro Jaya on July 28, 2004, though not widely documented, marked the beginning of the current efforts by the Cyber Crime unit. A significant case was the exposure of the online prostitution website wanita18.com in November 2008. The suspect, Albert Timotius, was arrested for offering prostitution services via the internet since 2005. This case outlined the misuse of technology for cybercrimes such as pornography and online prostitution,[9] and various other cybercrime cases.

Cybercrime, also known as computer crime, refers to criminal acts carried out using computer equipment within cyberspace or the internet to commit financial gain.[10] These acts include deceiving or defrauding the public, hacking

---

7 Fatmawati, "Kajian Kritis Terhadap Media Sosial Sebagai ' Tuhan Kedua ' Bagi Para Netizen," *Jurnal Pendidikan Sejarah Dan Sosiologi* 1 (2019).

8 and Antonia Merzon. Bandler, John, *Cybercrime Investigations: A Comprehensive Resource for Everyone*, *CRC Press*, 2020, https://doi.org/https://doi.org/10.1201/9781003033523.

9 Rahyadu Maulana Husada Raihan Khoerunisa, Inkcrah Prudensia, "Cybersex Dan Cyberpornography Studi Kasus Putusan PN Bekasi Nomor 76/Pid.Sus/2021/PN.Bks Raihan," *De Juncto Delicti* 2, no. 41 (2022): 14–22.

10 M. Chairul Basrun Umanailo et al., "Cybercrime Case as Impact Development of Communication Technology That Troubling Society," *International Journal of Scientific and Technology Research* 8, no. 9 (2019): 1224–28, https://www.ijstr.org/final-print/sep2019/Cybercrime-Case-As-Impact-Development-Of-Communication-Technology-That-Troubling-Society.pdf.

people's accounts, or breaching national information systems.[11] This act is carried out by a handful of people who use it for personal benefit and to the detriment of others.[12] Cybercrime uses the internet as a medium for tapping, stealing, and even damaging. Therefore, it is considered a modern phenomenon in criminal acts where the perpetrators are a step ahead of law enforcement.[13] Many users are not aware of the dangerous sites that exist on social media, coupled with several characteristics of long-distance communication with unlimited time such as WhatsApp, Twitter, Facebook, Instagram, Telegram, and similar apps. The presence of social media also influences perceptions of social status and has the potential to distort many existing thoughts and theories.[14]

Based on the type of activity, cybercrime is classified as unauthorised access to computer service systems, illegal content, data falsification, sabotage, and cyber extortion.[15] This correlates with the study[16] affirming that only illegal acts violating the law fall into the category of criminal offences, such as violations of intellectual property rights, privacy, hacking, and identity theft. Consequently, the use of identity-connected features or content that can identify individuals becomes an important part of gathering, preventing, and anticipating cyber activities. A key element on social media that aids in identification is the use of hashtags (#). The hashtag feature is becoming increasingly popular and serves as an indicator of standard responses to mass communication media, both globally and locally. Moreover, the use of #Cybercrime is an interesting indicator to be studied and examined in identifying cases of cybercrime and the intensity and activity of social media users around the topics. On Twitter, the hashtag #Cybercrime is analysed by examining the content that signals cyber activities. The trend in Indonesia continues to grow, and while technology enables the rapid transmission of information,[17] there is a need for a robust legal framework that strengthens the security system against cybercrime on social media platforms.

---

11 Andri Winjaya Laksana, "Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif," *Jurnal Hukum* 35, no. 1 (June 2, 2019): 52, https://doi.org/10.26532/jh.v35i1.11044.

12 Sutijono and Dimas Ardika Miftah Farid, "Cyber Counseling Di Era Generasi Milenial," *Sosio Humanika* 11, no. 1 (2018): 3–4.

13 Jangirala Srinivas, Ashok Kumar Das, and Neeraj Kumar, "Government Regulations in Cyber Security: Framework, Standards and Recommendations," *Future Generation Computer Systems* 92, no. 1 (2019): 178–88, https://doi.org/10.1016/j.future.2018.09.063.

14 Gomgom TP Siregar and Sarman Sinaga, "The Law Globalization in Cybercrime Prevention," *International Journal of Law Reconstruction* 5, no. 2 (2021): 211, https://doi.org/10.26532/ijlr.v5i2.17514.

15 Tarigan et al., "Cybercrime Case on Social Media in Indonesia."

16 Tolkah Tolkah, "Customary Law Existency in The Modernization of Criminal Law in Indonesia," *Varia Justicia* 17, no. 1 (May 7, 2021): 72–89, https://doi.org/10.31603/variajusticia.v17i1.5024.

17 I Nyoman Sukayasa and Wayan Suryathi, "Law Implementation of Cybercrime in Indonesia," *SOSHUM : Jurnal Sosial Dan Humaniora* 8, no. 2 (2018): 123–30, https://doi.org/10.31940/soshum.v8i2.985.

Cybercrime is a serious crime that requires a prompt response. The damages it causes are not limited to financial loss but also extend to moral and behavioural decline.[18] Therefore, the scope of the prevention is broad, making the study important for identifying content related to cybercrime through the trending hashtag #Cybercrime in Indonesia. It also aims to examine evolving legal frameworks in response to crimes in the digital era. Studies on cybercrime in Indonesia have primarily focused on normative legal aspects or case studies, without utilising social media-based big data content analysis. This presents a significant gap in the legal and digital criminology literature, particularly considering that social media serves as a primary platform for the dissemination and documentation of various forms of cybercrime.

This study fills the gap by examining the dynamics of the hashtag #Cybercrime on Twitter. According to data from https://www.patrolisiber.id/ in 2024, the most frequently reported categories of cybercrime were 2,350 threats, 1,867 instances of gambling, and 840 cases of insults or defamation. Geographically, Java Island records the highest intensity of cases, followed by Sumatra and Kalimantan. Indonesia is among the top five countries with the largest number of social media users. It ranks sixth globally in terms of cyberattacks, with 36.6 million attacks recorded over the last three years.[19] Given the increasing trend of digital crime, it is essential to acknowledge that the Indonesian legal system still faces significant challenges in responding to these dynamics. The identified obstacles include limited digital infrastructure, inadequate competence among law enforcement officers in information technology, and a lack of legal awareness in the community. Therefore, a repressive, preventive, and educational legal approach is necessary to create a safe and fair digital space that protects people's digital rights.

Methods

This study employed qualitative methods to explain the phenomena that occurred, highlighting holistic and contextual aspects,[20] describing analysis activities, and identifying key issues related to the impacts.[21] It focused on

[18] Adi Ahmad, Riyan Maulana, and Muhammad Yassir, "Cybersecurity Challenges In The Era Of Digital Transformation A Comprehensive Analysis Of Information Systems."

[19] Marianna Lezzi, Mariangela Lazoi, and Angelo Corallo, "Cybersecurity for Industry 4.0 in the Current Literature: A Reference Framework," *Computers in Industry* 103 (December 2018): 97–110, https://doi.org/10.1016/j.compind.2018.09.004; Akamai Technologies, "Akamai Research: Web Attacks Up 33%, APIs Emerge as Primary Targets" (Cambridge, 2025), https://www.akamai.com/newsroom/press-release/akamai-research-web-attacks-up-33-apis-emerge-as-primary-targets#:~:text=The majority of AI-powered,the second most attacked sector).

[20] Alison B. Hamilton and Erin P. Finley, "Qualitative Methods in Implementation Research: An Introduction," *Psychiatry Research* 280 (2019): 112516, https://doi.org/10.1016/j.psychres.2019.112516.

[21] Kristi Jackson and Patricia Bazeley, *Qualitative Data Analysis with NVivo*, 3rd ed. (SAGE Publications, 2019).

#CyberCrime content in the digital era in Indonesia, examining six stages of literature review through big data analysis, specifically identifying models of social media users in the digital era. The data collection method used in this study was based on big data sourced from social media, websites, various reports, journalism sources, and other study-related documents.[22] Furthermore, data analysis was conducted using NVivo 12 Plus software, a qualitative data analysis (QDA) tool, to understand the media usage model within mass social communication platforms. The study process was shown in the flowchart (graph) provided.

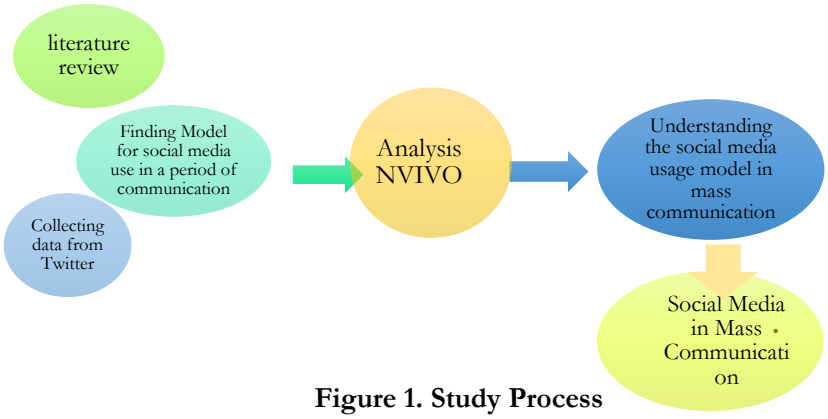

Figure 1. Study Process

Source: Researchers, 2024

The data were collected using the following methods: a literature review (document analysis), sourcing documents from news outlets, and the #CyberCrime Twitter page using the Ncapture feature for NVivoR1.7 via Google Chrome. Analysis was then conducted using the NVivo application, employing internet-based qualitative data methods, including data management, coding, validity and reliability testing, thematic analysis, interpretive and cross-case analysis, as well as visualisation of data analysis results (**Figure 1**). The study also explored word frequency, attributes, and cases from big data to generate factor and sub-factor categories relevant to the analysis.[23] NVivo remained a QDA tool used among authors globally.[24]

[22] Omotayo Olubiyi et al., "A Qualitative Case Study of Employee Turnover in Retail Business," *Heliyon* 5, no. 6 (2019): e01796, https://doi.org/10.1016/j.heliyon.2019.e01796.

[23] Shalin Hai-Jew, "NVivo 12 Plus's New Qualitative Cross-Tab Analysis Function," *C2C Digital Magazine* 1, no. 10 (2020): Article 15., https://scholarspace.jccc.edu/c2c_online/vol1/iss10/15.

[24] Maureen O'Neill, Sarah Booth, and Janeen Lamb, "Using NVivo™ for Literature Reviews: The Eight Step Pedagogy (N7+1)," *The Qualitative Report* 23, no. 13 (March 6, 2018): 21–39, https://doi.org/10.46743/2160-3715/2018.3030.

Results and Discussions

Cybercrime represented a dark side of internet-based communication technology, carrying wide-ranging implications across various aspects of life and is closely connected to organised crime. According to the 10th United Nations Congress held in Vienna, hacking was identified as the first form of cybercrime that required urgent attention and preventive action.

Cyber Activities against the Spread of #Cybercrime

Figure 2. Hashtags Clustered by Word Frequency Query Result
Source: *Coding Analysis through NVivoR12Plus Software*

Figure 2, presents a word cloud showing various hashtags related to cybersecurity issues. The size of each hashtag reflected its frequency and impact in public discussions, particularly on social media. Hashtags such as #cybercrime and #cybersecurity stood out prominently, showing significant attention and emotional responses connected to data theft, cyberattacks, and privacy violations. This visualisation emphasised that cybersecurity issues were a primary public concern and required serious attention from both the public and policymakers.

Table 1. Sentiment Analysis for #Cybercrime

Reference	Moderately negative	Very negative	Total
Reference Type = Web Page (1)	77.62%	22.38%	100%
Total (1)	77.62%	22.38%	100%

Sources: Coding Analysis through NVivo12Plus Software

Based on the results of the Word Frequency Query using NVivo RI.7, the results showed that mass communication was the primary target of cybercrime interaction with the public. The use of #cybercrime served as a form of feedback from the masses via social media, functioning both as an informational tool and a means to identify the evolving forms of cybercrime on these platforms. The impact of #cybercrime on social media, particularly Twitter, showed a strong influence on the level of cybercrime-related discourse. The frequency of tweets

or retweets containing #cybercrime significantly affected public social behaviour regarding cyber issues. Additionally, the dominant frequency of words related to #cybercrime showed a higher usage rate than those related to #cybersecurity. The sentiment analysis presented in Table 1 revealed a strong tendency to use #cybercrime, with a classification of 22.38% as highly negative and 77.62% as moderately negative. This suggested that tweets or content under the hashtag typically carried negative tones.

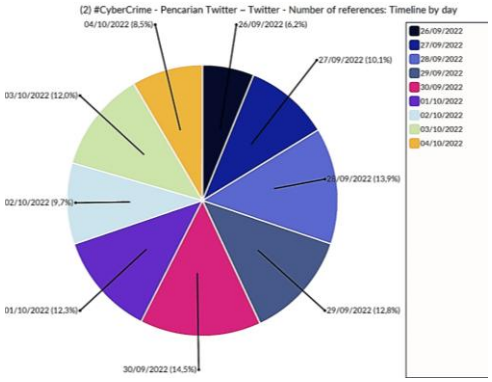

Figure 3. Twitter Activity Intensities

Sources: Coding Analysis through NVivo12Plus Software (Timeline by day)

Social media, particularly Twitter, serves as a mass communication tool to provide information backed by big data, as evidenced by the intensity of its activity. **Figure 3**, extracted using NVivo 12 Plus, visualises Twitter data based on the #cybercrime hashtag, displaying it along a daily timeline. The results showed that from September 26 to October 4, 2022, the intensity of #cybercrime remained high, indicating continuity in the use of the hashtag. It served as a prominent tool for information dissemination, reflecting how the digital era addressed cybercrime through social media engagement.

Cybercrime Cases and Reports

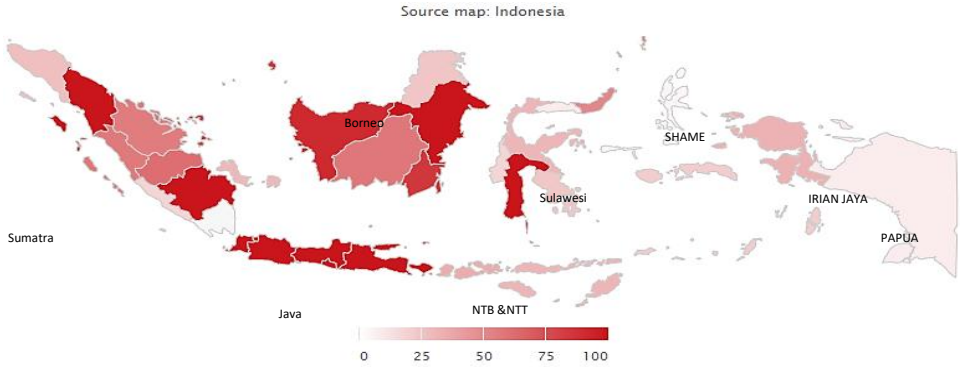

Figure 4. Cybercrime Cases by Location

Sources: NvivoR12 Plus Software &https://www.patrolisiber.id/

Table 2. Number of Reports of Cybercrime Cases in Indonesia 2024

Indicator	Value
Child Porn	**4**
Hoax/Fake news	**15**
Criminal	**69**
Forgery of Letters/Documents	**36**
Threats	**2350**
Humiliation/Defamation	**840**
Blasphemy	**8**
Selling illegal drugs on the internet, social media, or other social networks	**2**
Protected Animal Trade	**0**
People Trafficking	**3**
Gambling	**1867**
Provocation / Incitement	**25**
Others	**333**

Sources: https://www.patrolisiber.id/

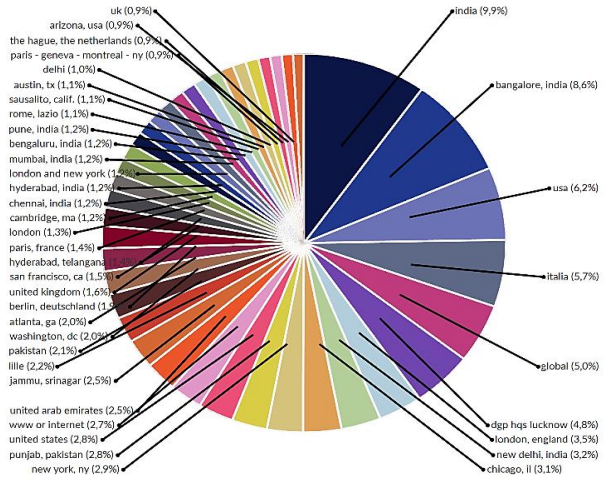

Figure 5. Reports of Cyber Crime Cases in Indonesia 2024 by Big Data
Sources: NvivoR1.7 Software &https://www.patrolisiber.id/

The results showed that globally, cybercrime cases analysed using NVivo R1.7 against the use of the #cybercrime hashtag suggested that the location with the highest number of cases in the world was India, at 9.9%, followed by Bangalore, India, at 8.9%, the USA, at 6.2%, and Italy, at 5.7%. The lowest figures were recorded in the UK, Arizona (USA), The Hague (Netherlands), Paris, Geneva, and Montreal, each with a rate of 0.9%, as shown in **Figure 5**. For Indonesia, the highest number of cases occurred on Java Island (outlined in red), followed by Sumatra, Kalimantan, Sulawesi, Irian Jaya, NTB & NTT, Maluku, and finally Papua, as shown in **Figure 4.**[25] The results also showed that case reports in

[25] Kai Wan Yuen et al., "A Comprehensive Database of Indonesian Dams and Its Spatial Distribution," *A Functional Biology of Sticklebacks* 15, no. 925 (2023): 4–19, https://doi.org/10.2307/jj.8306147.7.

Indonesia were categorised into 11 complaint indicators, ranging from Child Pornography to Other cases, as presented in **Table 2.** The data showed that the highest reported crime was threats, with 2,350 cases, followed by online gambling with 1,867. Cases with no recorded reports included protected animal trade, while the lowest figures were human trafficking (three cases) and illegal drug sales via the internet and social media (two cases).

Regarding cybercrime, the anonymity of the crime made it easier for cybercriminals to avoid detection and use chat rooms, Twitter, Facebook, and other open online discussion forums. The results showed that the use of #cybercrime was the primary and dominant indicator, with numerous associated content reflecting moderate negative sentiment, indicating public concern over cybercrime activities on Twitter.[26]

Social life, specifically protection, was portrayed in the media as a reflection of the balance in social relations and evolving public institutions, comprising values, attitudes, and behavioural patterns within society. Furthermore, sentiment analysis showed that content tagged with #cybercrime tended to focus on negative issues. The hashtag remained widely used as a platform for sharing information and reacting to the widespread occurrence of cybercrimes in the digital age, particularly through social media platforms such as Twitter, Facebook, Instagram, WhatsApp, and other digital networks.

The results showed that the digital era has had a significant impact on human survival, particularly in the protection of personal data, encompassing domains such as security and human rights protection. This was essential for avoiding criminal acts that threatened people, families, and the broader social environment. Currently, Indonesia can be categorised as a country with a reasonably high crime rate, involving various types of computer-related criminal activities. Jiushu outlined threats via text messages, commonly referred to as Flaming, as part of cybercrime.[27] This also correlated with the analysis[28], where cybercrimes could be carried out by hackers, interfering with personal activities, including hate speech and various inappropriate words, and occasionally escalating to direct threats.[29] Another growing issue was online gambling, a new trend that made it easier for cybercriminals to operate.[30]

In a widely reported Indonesian online gambling case, 329 accounts were analysed, with 202 accounts identified and blocked, and suspects classified as

---

26 Ida Musofiana, "Legal Protection For Victims Of Cybercrime In The Digital Era In Strengthening Cyber Democracy In Indonesia Post 2019 General Election.," *In The 2nd International Conference And Call Paper* 1, no. 1 (2021): 84–90.

27 Jiushu Xie et al., "When Humanity Fades: The Chain Roles of Self-Dehumanization and Empathy in Cyberostracism-Flaming Link," *Current Psychology* 44, no. 11 (June 5, 2025): 10336–47, https://doi.org/10.1007/s12144-025-07890-0.

28 Sutijono and Farid, "Cyber Counseling Di Era Generasi Milenial."

29 Bandler, John, *Cybercrime Investigations: A Comprehensive Resource for Everyone.*

30 CNBC, "Tersangka Kasus Judi Online Kelas Atas," 2022.

high-stakes gamblers. This underscored the seriousness of cybercrime in Indonesia, confirming the need for proper and urgent attention to the issue. The challenges arising from the intersection of law, technology, and globalisation pointed to humanity. Legal frameworks should not only remain normative but should also reflect human-centred values, as people are considered social beings.[31] The evolution of cybercrime posed a major threat to both society and governmental stability.[32] Therefore, the government was expected to respond swiftly and decisively to criminal threats in the digital age. Particular attention should be paid to digital security, particularly in relation to the rule of law, because the law serves as a crucial tool for regulating and protecting human beings. In the current digital environment, this correlated with the understanding that the purpose of the law was to promote peaceful interpersonal relationships.

Cybercrime Regulations in Indonesia

In Indonesia, the evolution of regulation within the national legal system contributed to scientific and legal progress, particularly in addressing criminal cases in society. To assess the enforcement of cybercrime-related legal provisions, a concrete case that served as an example was the Muhammad Kace case in 2021.[33] Muhammad Kace, a former pastor who later converted to Islam, uploaded several videos on his YouTube channel containing elements of hate speech and blasphemy. The content was considered offensive to certain religious groups and triggered public unrest. Consequently, law enforcement officers applied articles in the Electronic Information and Transactions Law (UU ITE) Number 11 of 2008, specifically Article 28 paragraph (2) and Article 45A paragraph (2), which regulated the prohibition of the dissemination of information inciting hatred based on SARA (ethnicity, religion, race, and inter-group relations).

Additionally, Article 156a of the Criminal Code concerning blasphemy was also used as a legal basis.[34] The legal process took place through the digital forensic investigation of the suspect's electronic devices and social media

[31] Herowati Sitorus, "Pemahaman Generasi Millenial Terhadap Hak Asasi Manusia: Studi Hak Asasi Manusia Menurut Alkitab," *Jurnal Christian Humaniora* 4, no. 1 (2020): 93–103, https://doi.org/10.46965/jch.v4i1.153.

[32] M Irfan et al., "Analyzes of Cybercrime Expansion in Indonesia and Preventive Actions," *IOP Conference Series: Materials Science and Engineering* 434 (December 3, 2018): 012257, https://doi.org/10.1088/1757-899X/434/1/012257.

[33] Handar Subhandi Bakhtiar et al., "The Utilisation of Scientific Crime Investigation Methods and Forensic Evidence in the Criminal Investigation Process in Indonesia," *Egyptian Journal of Forensic Sciences* 15, no. 1 (May 29, 2025): 39, https://doi.org/10.1186/s41935-025-00456-y.

[34] Ayub Mursalin, "Indonesian Blasphemy Laws and the Gradual Shrinking of the Domain of Religious Freedom since 1965," *Archipel* 98 (2019): 151–76, https://doi.org/10.4000/archipel.1349.

accounts. Consequently, Muhammad Kace was found guilty and sentenced to 10 years in prison.[35]

The case showed that Indonesia had existing legal instruments capable of effectively prosecuting cybercrimes based on hate speech. Despite the importance of digital forensics in the evidence-gathering process, significant challenges remained, including limited facilities, inadequate infrastructure, and a shortage of competent human resources in information technology among law enforcement officers.[36] Additionally, low public legal awareness and the rapid spread of digital information posed further obstacles to effective law enforcement. Although regulations were available, there was a pressing need to strengthen institutional aspects, increase digital literacy, and develop reliable human resources to ensure that cybercrime enforcement in Indonesia operated optimally and adapted to technological advancements.

Analysis of Digital Forensics Development in Cybercrime Investigation in Indonesia

The provisions of criminal law against cybercriminals in Indonesia were outlined in Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), specifically Articles 27 to 52, which formed the legal framework for addressing cybercrime. These articles regulated various acts that were prohibited in the digital space, including the distribution of content violating morality, defamation, the spread of fake news, hate speech, blackmail, threats, and unauthorised access to electronic systems. For example, Article 27 prohibited the distribution of pornographic and insulting content through electronic media, while Article 28 took action against the spread of hoaxes and hate speech based on SARA.

Furthermore, Articles 30 to 37 regulated the prohibition of hacking systems, stealing data, and spreading viruses or malicious programs. Articles 38 to 52 further contained provisions related to system security, the responsibility of electronic system organisers, and the authority of law enforcement officers in investigating and prosecuting violations. The latest revision, through Law Number 1 of 2024, clarified several provisions that were previously open to multiple interpretations, including the addition of Articles 27A and 27B, which more specifically regulated defamation and electronic extortion. Based on this change, the ITE Law was expected to provide fairer and more proportional legal protection in controlling people's behaviour in the digital world, without sacrificing freedom of expression.

---

35 Siti Rahayu Selamat et al., "Traceability in Digital Forensic Investigation Process," in *2011 IEEE Conference on Open Systems* (IEEE, 2011), 101–6, https://doi.org/10.1109/ICOS.2011.6079259.

36 Nur Iman, Aris Susanto, and Rahmat Inggi, "Analysis of the Development of Digital Forensics in Cybercrime Investigations in Indonesia (Systematic Review)," *Jurnal Telekomunikasi Dan Komputer* 9, no. 3 (2020): 186, https://doi.org/10.22441/incomtech.v9i3.7210.

The international response to cybercrime was reflected in discussions on high-tech crime at several United Nations conferences. These included (1) the United Nations Conference on Crime Prevention and Treatment of Offenders,[37] (2) The Bangkok Declaration on Synergy and Response: Strategic Partnerships in Crime Prevention and Criminal Justice, (3) The 12th United Nations Conference on Crime Prevention and Criminal Justice. These conferences recognised cyber-crime as an evolving form of crime that still faced numerous legal and institutional challenges. The disturbances included (1) limited expertise in digital forensics and electronic surveillance, (2) low capacity and insufficient technical tools among law enforcement agencies, (3) inadequate infrastructure and facilities, (4) difficulty in identifying victims, and (5) weak legal awareness among the public.

The development of communication technology, including social media and internet usage, has fundamentally changed various aspects of social life, such as industry, economy, education, and even human interaction patterns.[38] Activities that were previously carried out in person shifted to the virtual space through digital networks, erasing the boundaries of space and time.[39] This phenomenon also shaped the minds and personalities of the people, creating a new, dynamic social reality. During this progress, serious challenges evolved in the form of increasingly complex cybercrime. In examining the phenomenon, a legal sociology framework such as Eugen Ehrlich's "living law" theory became relevant. Ehrlich had emphasised that living law in society did not correlate with written law.[40]

The discrepancy created a gap between the ideal legal norms and the factual implementation in the field. In the context of cybercrime, that gap was reflected in weak law enforcement, often due to law enforcement officers' limited understanding of technology, a lack of adaptive regulations, or jurisdictional constraints arising from the cross-border nature of digital crime. In Indonesia, efforts to address this challenge were marked by the introduction of a new legal system through the ITE Law No. 11 of 2008, which was later revised by Law No. 19 of 2016, and by Law No. 27 of 2022 concerning Personal Data Protection. However, its implementation still faced obstacles such as inadequate socialisation, inconsistent enforcement, and multiple interpretations of articles that were prone to misuse. The most prevalent forms of cybercrime at that time included phishing, hacking, online fraud, the spread of hoaxes, digital identity theft, content-based extortion (such as sextortion), and

---

37 Dewi Bunga, "Legal Response to Cybercrime in Global and National Dimensions," *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)* 06, no. 01 (April 2019): 69–89, https://doi.org/10.22304/pjih.v6n1.a4.

38 Llysselie Gay Querol Leiva, "Impact of Information and Communication Technologies on Everyday Life," *Management (Montevideo)* 3 (February 8, 2025): 130, https://doi.org/10.62486/agma2025130.

39 Epi Ludvik Nekaj, "The Crowd Economy," in *Digital Marketing and Consumer Engagement* (IGI Global, n.d.), 1513–31, https://doi.org/10.4018/978-1-5225-5187-4.ch076.

40 Ralf Seinecke, "Der Rechtsbegriff Des Lebenden Rechts," *Zeitschrift Für Rechtssoziologie* 44, no. 1 (May 7, 2024): 241–76, https://doi.org/10.1515/zfrs-2024-2003.

illicit transactions on the dark web. These crimes required a legal method that was not only repressive but also preventive and educational, enabling the public to develop awareness and secure legal protection in the digital space in a sustainable manner.

Cybercrime has become a real and serious global threat to both national and international security. The rapid development of communication and internet technology opened enormous opportunities for criminals to carry out their actions without being hindered by geographical boundaries and with a high level of anonymity.[41] In that context, cybercrime was categorised as a global disaster because its impact was not only detrimental to people but could also disrupt the economic, social, and political stability of a country. Crimes such as data hacking, online fraud, hate speech, and gambling became increasingly rampant, posing major challenges in the digital era. Cybercrime was not only a legal issue but also raised broader humanitarian concerns, as it threatened fundamental human rights, including privacy, security, and safety.

Therefore, a comprehensive and adaptive legal approach was needed to address the dynamics of technology, encompassing responsive regulatory reform, enhancing law enforcement capacity, strengthening cybersecurity institutions, and facilitating international cooperation in eradicating cross-border cybercrime. Digital education and literacy for the community also had to be prioritised to increase awareness of cyber risks and establish a healthy digital culture. Fair and humanistic law enforcement was also important to ensure that legal protection was not misused as a repressive tool but rather served as a protector of citizens' rights. Synchronisation between law, technology, and human values was considered crucial for achieving a safe and just social order during the ever-growing digital transformation, which aligns with the study's objectives on the impact of social media and community protection in the digital era.

Conclusions

In conclusion, the analysis of #cybercrime content using NVivo12 Plus showed measurable effectiveness in achieving the objectives. This study analysed Twitter accounts that used the hashtag #cybercrime, and the results showed a significant impact, effectively describing cyber-related activities. The role of information technology in mass communication, particularly in the use of #cybercrime, was significantly active in 2022. Cybercrimes have been identified across various regions globally, particularly in India, the USA, and Indonesia, with high rates of cybercrime, including Java and Sumatra. The most commonly reported cases were threats and online gambling, while illegal protected animal trade remained largely unreported. Regarding legal, technological, and digitalisation issues, Indonesia still requires significant improvement, specifically in the legal framework and its enforcement. Considering that cybercrime is a serious crime,

[41] Bunga, "Legal Response to Cybercrime in Global and National Dimensions."

both the public and law enforcement agencies need to reevaluate existing mechanisms to combat it effectively. Analysis of #cybercrime content showed that cybercrime persisted in various forms and modes. At the same time, the new legal system introduced in the digital era had not fully accommodated the complexities of cybercrime. Numerous obstacles were identified in the area of investigation and legal instruments, which continued to hinder effective law enforcement against cybercrime in Indonesia.

Acknowledgements

Sincere gratitude and pride were expressed to the team for unwavering support and dedication throughout the preparation of this article. Appreciation was also extended to the Faculty of Sharia, UIN Sulthan Thaha Saifuddin Jambi, for support in the completion of this paper. Lastly, thanks and acknowledgements were given to all individuals and institutions that contributed to and assisted in the successful execution of this study.

References

Adi Ahmad, Riyan Maulana, and Muhammad Yassir. "Cybersecurity Challenges In The Era Of Digital Transformation A Comprehensive Analysis Of Information Systems." *Journal Informatic, Education and Management (JIEM)* 6, no. 1 (2024): 7–11. https://doi.org/10.61992/jiem.v6i1.57.

APJII. "Survei Pengguna Internet Indonesia." APJII, 2020.

Bahri, Saiful. "Communication Strategies in Building Public Trust Based on Cyber Public Relations." *Proceeding of International Conference on Education, Society and Humanity* 2, no. 1 (2024): 535–46. https://ejournal.unuja.ac.id/index.php/icesh/article/view/7918.

Bakhtiar, Handar Subhandi, Amir Ilyas, Abdul Kholiq, and Handina Sulastrina Bakhtiar. "The Utilisation of Scientific Crime Investigation Methods and Forensic Evidence in the Criminal Investigation Process in Indonesia." *Egyptian Journal of Forensic Sciences* 15, no. 1 (May 29, 2025): 39. https://doi.org/10.1186/s41935-025-00456-y.

Bandler, John, and Antonia Merzon. *Cybercrime Investigations: A Comprehensive Resource for Everyone*. *CRC Press*, 2020. https://doi.org/https://doi.org/10.1201/9781003033523.

Bunga, Dewi. "Legal Response to Cybercrime in Global and National Dimensions." *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)* 06, no. 01 (April 2019): 69–89. https://doi.org/10.22304/pjih.v6n1.a4.

CNBC. "Tersangka Kasus Judi Online Kelas Atas," 2022.

Ellyona Putri, Kadek Devina, Mariano Wawan Latbin, and Gerald Aldytia Bunga. "Phenomenom Cyber Crime in Indonesia in the Digitalization Era." *Journal of Digital Law and Policy* 3, no. 2 (2024): 99–109. https://doi.org/10.58982/jdlp.v3i2.549.

Fatmawati. "Kajian KritisTerhadap Media Sosial Sebagai 'Tuhan Kedua' Bagi Para Netizen." *MAHARSI* 1, no. 01 (February 28, 2019): 89–98. https://doi.org/10.33503/maharsi.v1i01.358.

Gay Querol Leiva, Llysselie. "Impact of Information and Communication Technologies on Everyday Life." *Management (Montevideo)* 3 (February 8, 2025): 130. https://doi.org/10.62486/agma2025130.

Hai-Jew, Shalin. "NVivo 12 Plus's New Qualitative Cross-Tab Analysis Function,." *C2C Digital Magazine* 1, no. 10 (2020): Article 15. https://scholarspace.jccc.edu/c2c_online/vol1/iss10/15.

Hakim, Lukmanul, Tien F. Kusumasari, and Muharman Lubis. "Text Mining of UU-ITE Implementation in Indonesia." *Journal of Physics: Conference Series* 1007, no. 1 (2018). https://doi.org/10.1088/1742-6596/1007/1/012038.

Hamilton, Alison B., and Erin P. Finley. "Qualitative Methods in Implementation Research: An Introduction." *Psychiatry Research* 280 (2019): 112516. https://doi.org/10.1016/j.psychres.2019.112516.

Iman, Nur, Aris Susanto, and Rahmat Inggi. "Analysis of the Development of Digital Forensics in Cybercrime Investigations in Indonesia (Systematic Review)." *Jurnal Telekomunikasi Dan Komputer* 9, no. 3 (2020): 186. https://doi.org/10.22441/incomtech.v9i3.7210.

Irfan, M, M A Ramdhani, W Darmalaksana, A Wahana, and R G Utomo. "Analyzes of Cybercrime Expansion in Indonesia and Preventive Actions." *IOP Conference Series: Materials Science and Engineering* 434 (December 3, 2018): 012257. https://doi.org/10.1088/1757-899X/434/1/012257.

Jackson, Kristi, and Patricia Bazeley. *Qualitative Data Analysis with NVivo*. 3rd ed. SAGE Publications, 2019.

Laksana, Andri Winjaya. "Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif." *Jurnal Hukum* 35, no. 1 (June 2, 2019): 52. https://doi.org/10.26532/jh.v35i1.11044.

Lezzi, Marianna, Mariangela Lazoi, and Angelo Corallo. "Cybersecurity for Industry 4.0 in the Current Literature: A Reference Framework." *Computers in Industry* 103 (December 2018): 97–110. https://doi.org/10.1016/j.compind.2018.09.004.

Mursalin, Ayub. "Indonesian Blasphemy Laws and the Gradual Shrinking of the Domain of Religious Freedom since 1965." *Archipel* 98 (2019): 151–76. https://doi.org/10.4000/archipel.1349.

Musofiana, Ida. "Legal Protection For Victims Of Cybercrime In The Digital Era In Strengthening Cyber Democracy In Indonesia Post 2019 General Election." *In The 2nd International Conference And Call Paper* 1, no. 1 (2021): 84–90.

Nekaj, Epi Ludvik. "The Crowd Economy." In *Digital Marketing and Consumer Engagement*, 1513–31. IGI Global, n.d. https://doi.org/10.4018/978-1-

5225-5187-4.ch076.

O'Neill, Maureen, Sarah Booth, and Janeen Lamb. "Using NVivo™ for Literature Reviews: The Eight Step Pedagogy (N7+1)." *The Qualitative Report* 23, no. 13 (March 6, 2018): 21–39. https://doi.org/10.46743/2160-3715/2018.3030.

Olubiyi, Omotayo, Garrett Smiley, Henry Luckel, and Ralph Melaragno. "A Qualitative Case Study of Employee Turnover in Retail Business." *Heliyon* 5, no. 6 (2019): e01796. https://doi.org/10.1016/j.heliyon.2019.e01796.

Raihan Khoerunisa, Inkcrah Prudensia, Rahyadu Maulana Husada. "Cybersex Dan Cyberpornography Studi Kasus Putusan PN Bekasi Nomor 76/Pid.Sus/2021/PN.Bks Raihan." *De Juncto Delicti* 2, no. 41 (2022): 14–22.

Seinecke, Ralf. "Der Rechtsbegriff Des Lebenden Rechts." *Zeitschrift Für Rechtssoziologie* 44, no. 1 (May 7, 2024): 241–76. https://doi.org/10.1515/zfrs-2024-2003.

Selamat, Siti Rahayu, Robiah Yusof, Shahrin Sahib, Nor Hafeizah Hassan, Mohd Faizal Abdollah, and Zaheera Zainal Abidin. "Traceability in Digital Forensic Investigation Process." In *2011 IEEE Conference on Open Systems*, 101–6. IEEE, 2011. https://doi.org/10.1109/ICOS.2011.6079259.

Siregar, Gomgom TP, and Sarman Sinaga. "The Law Globalization in Cybercrime Prevention." *International Journal of Law Reconstruction* 5, no. 2 (2021): 211. https://doi.org/10.26532/ijlr.v5i2.17514.

Sitorus, Herowati. "Pemahaman Generasi Millenial Terhadap Hak Asasi Manusia: Studi Hak Asasi Manusia Menurut Alkitab." *Jurnal Christian Humaniora* 4, no. 1 (2020): 93–103. https://doi.org/10.46965/jch.v4i1.153.

Srinivas, Jangirala, Ashok Kumar Das, and Neeraj Kumar. "Government Regulations in Cyber Security: Framework, Standards and Recommendations." *Future Generation Computer Systems* 92, no. 1 (2019): 178–88. https://doi.org/10.1016/j.future.2018.09.063.

Sukayasa, I Nyoman, and Wayan Suryathi. "Law Implementation of Cybercrime in Indonesia." *SOSHUM : Jurnal Sosial Dan Humaniora* 8, no. 2 (2018): 123–30. https://doi.org/10.31940/soshum.v8i2.985.

Sutijono, and Dimas Ardika Miftah Farid. "Cyber Counseling Di Era Generasi Milenial." *Sosio Humanika* 11, no. 1 (2018): 3–4.

Tarigan, Vita Cita Emia, Lidya Rahmadani Hasibuan, Rahima br Purba, Irawan, Pipit Buana Sari, Yossie Rossanty, and Muhammad Dharma Tuah Putra Nasution. "Cybercrime Case on Social Media in Indonesia." *International Journal of Civil Engineering and Technology* 9, no. 7 (2018): 783–88. https://iaeme.com/Home/article_id/IJCIET_09_07_081.

Technologies, Akamai. "Akamai Research: Web Attacks Up 33%, APIs Emerge as Primary Targets." Cambridge, 2025.

https://www.akamai.com/newsroom/press-release/akamai-research-web-attacks-up-33-apis-emerge-as-primary-targets#:~:text=The majority of AI-powered,the second most attacked sector).

Tolkah, Tolkah. "Customary Law Existency in The Modernization of Criminal Law in Indonesia." *Varia Justicia* 17, no. 1 (May 7, 2021): 72–89. https://doi.org/10.31603/variajusticia.v17i1.5024.

Umanailo, M. Chairul Basrun, Imam Fachruddin, Deviana Mayasari, Rudy Kurniawan, Dewien Nabielah Agustin, Rini Ganefwati, Pardamean Daulay, et al. "Cybercrime Case as Impact Development of Communication Technology That Troubling Society." *International Journal of Scientific and Technology Research* 8, no. 9 (2019): 1224–28. https://www.ijstr.org/final-print/sep2019/Cybercrime-Case-As-Impact-Development-Of-Communication-Technology-That-Troubling-Society.pdf.

Xie, Jiushu, Yun Lian, Zixin Liu, Wenli He, and Zihan Yin. "When Humanity Fades: The Chain Roles of Self-Dehumanization and Empathy in Cyberostracism-Flaming Link." *Current Psychology* 44, no. 11 (June 5, 2025): 10336–47. https://doi.org/10.1007/s12144-025-07890-0.

Yuen, Kai Wan, Edward Park, Melda Hazrina, Muh Taufik, Edgardo Latrubesse, and Janice Ser Huay Lee. "A Comprehensive Database of Indonesian Dams and Its Spatial Distribution." *A Functional Biology of Sticklebacks* 15, no. 925 (2023): 4–19. https://doi.org/10.2307/jj.8306147.7.