Jurnal Tana Mana
Vol. 6 No. 1, April 2025
https://ojs.staialfurqan.ac.id/jtm/

The Progression of Cybercrime within the Context of Criminal Law Literature: Theoretical Framework and Practical Implications in Indonesia

Apitta Fitria Rahmawati [1*], Yuris Tri Naili [1]
[1] *Universitas Harapan Bangsa, Indonesia*

apittafitriarahmawati@uhb.ac.id*

Abstract

The This study examines the development of the concept of cybercrime in the criminal law literature in Indonesia and analyzes the relationship between theories in criminal law literature and the practice of law enforcement against cybercrime in the Indonesian criminal justice system. This study was conducted using a normative legal research method, while the approach used is a conceptual approach to regulation and practice. The types and sources of data in this study are secondary data using data collection techniques with various references, including journals, books, documentation, the internet, and libraries. Qualitative data analysis techniques. The results of this study indicate that although criminal law literature has begun to respond to cybercrime, there are still some gaps between the construction of theory and the practice of handling cyber cases in the field. Several concepts such as the principle of legality, forms of error, and criminal liability still need to be adjusted to the characteristics of technology-based crimes. Therefore, it is necessary to update criminal law thinking that is more adaptive and responsive to the development of the times.

Keywords: Cybercrime, Criminal Law, Legal Literature, Theory and Practice

Diterbitkan oleh Fakultas Syariah Sekolah Tinggi Agama Islam (STAI) Al-Furqan Makassar
ISSN 2622-5212
Website https://ojs.staialfurqan.ac.id/jtm/

PENDAHULUAN

Indonesia is a rule-of-law country, according to Section 3 of Article One of the 1945 Constitutions of the Republic of Indonesia. The Constitution of the Republic of Indonesia from 1945 states in Article 28 D, paragraph (1) that "Everyone has the right to be acknowledged, assured, protected, and to equitable legal certainty" , as well as equal standing under the law." Indonesia must protect this right for its people as a rule-of-law state. One of these citizens' rights needs to be fulfilled in accordance with the evolution of more progressive times.The advancements in the contemporary globalization age facilitate many types of activity. Globalization is the process of entering the global domain with the goal of allowing mankind to meet its requirements with all of the conveniences available, which subsequently impacts changes in numerous elements of life within society.

In today's globalized world, the communication and technology industries are rapidly developing, and progress in many disciplines is increasing. The quick development of technology in the contemporary era has brought convenience to society in a variety of ways (Ginara et al., 2022). On the other side, technological advancement creates potential for some groups to exploit it for criminal reasons. Criminals often exploit information technology, particularly social media, to perpetrate cybercrime.

The government is interested in enacting laws that may be used to apprehend criminals in the digital realm right away due to the rising number of cybercrime cases, particularly in Indonesia. The Indonesian government has implemented the Cybercrime Law (Law Cyber) into Law No. 11 of 2008 on Electronic Data and Exchanges . It anticipates that this law will enable it to handle, suppress, and prevent criminal activity in the digital realm (Habibi & Liviani, 2020). Cybercrime is addressed in Indonesian criminal law by particular legislation, namely Law No. 11 of 2008 about Electronic Information and Transactions (ITE Law), as amended by Law No. 9 of 2016, and some articles in the Criminal Code (KUHP). Nonetheless, the complexities of cybercrime frequently

present obstacles in terms of evidence, jurisdiction, and law enforcement effectiveness. This highlights the limitations of conventional criminal law in tackling crimes related to digital technologies (Ginara et al., 2022).

In Indonesia, academic criminal law literature has begun to examine cybercrime as a legal issue that must be redefined in light of traditional criminal norms such as the principle of legality, forms of culpability, and criminal liability. However, it is unclear if the literature can provide a strong conceptual foundation for addressing the dynamics of cybercrime. There is a gap between theory in criminal law doctrine and law enforcement practice in the field, where police officers, prosecutors, and other law enforcement court frequently confront challenges in terms of digital evidence, jurisdiction, and technical capability limits (Sofian, 2021).

Data from the Indonesian National Police's Criminal Investigation Agency shows that up until 2025, over 17,000 cybercrime reports were filed, including 14,495 incidents of online fraud, 8,614 violent threats, 6,556 cases of defamation, 3,675 threats of defamation, and 2,880 other crimes (Basreskrim Polri, 2025). Online fraud, unauthorized access to computer systems, hate speech, the dissemination of pornographic material, and digital extortion are among the most prevalent data. These numbers demonstrate a notable rise over prior years, underscoring the significance of fortifying the criminal justice system to effectively address cyberthreats. Due to difficulties with digital evidence, ambiguous perpetrator identities, and cross-border jurisdictional restrictions, many of these cases are still unresolved.

The aforementioned case shows how Indonesian criminal law, which acts as a lex generalis, is still attempting to adjust to the evolution of crime in the digital age, which may be the reason for the high rate of cybercrime. Even while laws like Law Number 11 of 2008 governing Electronic Information and Transactions (ITE Law) and its amendments already exist, there are still a number of barriers to their implementation. The problem includes conflicting legal requirements, unclear article interpretation, and inadequacies in the way the law is enforced. The necessity to update methods in criminal law literature is highlighted by the rising prevalence of cybercrime and the ineffectiveness of existing legal sanctions. For legal theory to be a helpful guide for law enforcement actions in the Indonesian criminal justice system, which is quickly moving into the digital era, normative and contextual legal thinking is required.

In actuality, the requirements of that practice have not yet been entirely satisfied by Indonesian criminal law literature. When dealing with cyber concerns involving algorithms, global networks, or artificial intelligence, traditional concepts of criminal law such as the principle of legality, forms of culpability, and criminal accountability often become inflexible. These legal concepts' shortcomings cause a disconnect between scholarly theory and the demands of the real world. Cybercrime, on the other hand, necessitates a more sophisticated strategy that incorporates knowledge of technology and a variety of disciplines. In order to appropriately address the dynamics and patterns of constantly evolving digital crimes, it is crucial to update the current criminal law theoretical framework.

The most basic element, namely how the growth of cybercrime undermines and changes the theoretical underpinnings of criminal law itself, has not been covered in the majority of research. As a result, this study assesses the criminal law theoretical framework that supports Indonesia's regulation and enforcement of the law against cybercrime in addition to discussing the application of positive law. By offering a more thorough and in-depth conceptual approach, this study aims to close the gaps in the criminal law literature that have placed an undue emphasis on the practice of applying the law. The trajectory of national criminal law evolution in addressing the increasingly complex nature of digital crimes is also critically examined in this research.

METHOD

A sort of technique in legal research that is based on the analysis of applicable regulations and related to the legal concerns that are the primary focus of the study is the qualitative approach used in this study, which is juridical normative in character (Benuf et al., 2019). This approach was selected because its main goals are to assess the criminal law theory framework's applicability in addressing cyber advances and to look at how well the relevant positive legal norms are working.

Data collection in this research was conducted through literature study. Data collection was carried out by studying and/or exploring various journals, books, documents, and other data or information sources deemed relevant to the study (Supriyadi, 2017). The legal framework analyzed in this study is Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE

Law) along with its amendments through Law No. 9 of 2016. The research also involves field practices obtained from internet data source references.

RESULT AND DISCUSSION

The Development of Criminal Law Concepts in Responding to Cybercrime

The rise of cybercrime in Indonesia has sparked a variety of ideas and discussions among criminal law professors. The national criminal law literature, which previously paid little attention to the topic of technology-based crimes. However, as cybercrime has escalated and become more complicated, specialists have begun to propose conceptual methods aimed at harmonizing criminal principles and norms with digital world characteristics.

The phenomenon of cybercrime has evolved into a systemic legal issue that affects all levels of society. Many cybercrimes target government agencies, digital financial systems, and even the state's critical infrastructure. Cases such as personal data breaches, defacing government websites, and fraud through illicit online loan applications demonstrate the fragility of digital security mechanisms and the lagging legal framework(Kominfo, 2024).

Cybercrime is a criminal phenomena that has emerged as a logical result of advances in information technology. In Indonesia, cybercrime presents a significant challenge to the criminal justice system, which has always been intended to tackle traditional crimes. Although the Criminal Code (KUHP) remains the primary legal framework for criminal prosecution, many types of cybercrime are not specifically addressed in the KUHP due to their novel and highly technical character.

From a legal standpoint, Soedjono Dirdjosisworo stated that the social changes and technological advancements over the last five decades since 1985, along with the pace of social and technological development and the increasing influence of globalization driven by information and communication technology, clearly show that the Criminal Code has long been unable to fully accommodate and anticipate the growing, qualitatively and quantitatively increasing criminal actions with (Aldriano & Priyambodo, 2022).

The dynamics of cybercrime cases in Indonesia have changed significantly over time, reflecting the rising penetration of technology and internet access across all levels of society. Rapid improvements in the digital realm have opened spaces for the emergence of many types of cybercrime, such as online fraud, personal data theft, and cyberattacks on critical infrastructure (Syahrir et al., 2025).

Although Law Number 9 of 2016 amending Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) serves as the main legal framework for addressing cybercrime, various stakeholders argue that the normative content of the ITE Law remains expansive and fails to encompass the complete range of swiftly changing digital offenses. As a result, there is a discrepancy between the increasing complexity of cybercrime and law enforcement's limited effectiveness, which is confined by legislation, resources, and traditional criminal law concepts.

The occurrence of such innovations necessitates the reformulation of criminal law on the normative, institutional, and theoretical levels. Criminal law ideas such as the principle of legality, locus delicti, culpability, and criminal liability must be enlarged and reinterpreted to reflect the realities of digital crimes that are not limited by traditional geography and time.

Additionally, this study offers a methodical mapping of the distinctions between the traditional theories of criminal law that apply to the Indonesian legal system and the developments of contemporary ideas from across the world that are intended to tackle the intricacies of cybercrime. The approach to digital crime in Indonesian legal study is typically still normative in nature, i.e., the evaluation of laws like the Criminal Code and the ITE Law without critically examining the underlying criminal law theory concepts.

Accordingly, this study's primary contribution is its bravery in questioning whether existing criminal law theory is sufficient for describing, categorizing, and dealing with non-traditional types of cybercrime. By offering a comparative and thoughtful analysis of the necessity of reimagining the criminal justice system to become more contextual and relevant in the digital age, this study fills the knowledge gap. Although it is evident that the Criminal Code's regulations pertaining to cybercrime are still primarily general in nature, they are specifically regulated and arranged in accordance with the frequency of occurrence of these cases due to the potential

occurrence of cases in the virtual world and the classification of cybercrimes (Sugiaryo, 2010). This demonstrates how the philosophy of Indonesian criminal law has not yet fully included the idea of cybercrime.

Regarding the criminal code of Indonesia, the errors made by cybercriminals are frequently linked to the difficulties in establishing components of guilt and illegal activity. Because of the intricacy of the technology that can be employed in cybercrime, it is challenging for law enforcement to determine and validate the malevolent purpose and acts of the criminal (Aini & Lubis, 2024).

The idea of criminal liability is being introduced in criminal law literature, along with the usage of algorithmic systems and corporate liability. Because they have control systems over the digital platforms used for crimes, businesses can be directly held criminally liable in the cyber context, according to research by Eddy O.S. Hiariej (O.S, 2020) Aspects of technical proficiency, system mastery, and purpose (mens rea) pertinent to the offender's activities must also be taken into account when determining their liability.

Since cybercrime sometimes involves cross-regional and even cross-national activity, some literature also addresses the necessity for an update to the doctrine of locus delicti (the place where the crime happened). This calls for a revision of the Criminal Code's provisions pertaining to national legal jurisdiction and presents difficulties with regard to jurisdiction and international cooperation.

Therefore, it may be said that Indonesian criminal law literature demonstrates trends and advancements in combating cybercrime. Even though it is not yet completely systematic, theoretical progress is already moving in the direction of integrating traditional criminal rules with the flexible digital environment while maintaining the principles of fairness and legal reliability.

The inefficiency of applying criminal law theory to the practice of cyber law enforcement

Rapid advancements in digital technology have led to a constant evolution in cybercrime tactics, creating new difficulties for law enforcement. Despite its 2016 revision, the ITE Law still does not completely address a number of more sophisticated cybercrimes, such as the use of artificial intelligence in cyberattacks or the dissemination of malware in novel ways (Salsabilla & Angelina, 2024).

Indonesian criminal law literature has established a solid theoretical foundation for the notions of offenses, criminal liability, and essential principles like legality and culpability. However, it is possible that when these principles are met with the reality of cybercrime, which is dynamic, multinational, and difficult to detect, a gap between theory and practice would emerge.

First, This viewpoint is consistent with the KUHP's legality principle, which is stated explicitly in Article I, paragraph (1), "There is no crime 'nulla poena sine lege poenali praevia,'" or, to put it another way, "no punishment without a prior law." In general, cybercriminals have committed crimes, particularly since Law No. 11 of 2008 was passed (Mewengkang et al., 2021).

In essence, the legality principle is understood as follows: first, no action is forbidden and subject to punishment until it is specified in a law; second, each prohibited act must be explicitly mentioned in the criminal offense's formulation; and third, laws It is forbidden to apply penalties retroactively. According to Article 1 paragraph (1) of the Criminal Code, the meaning is the formal legality concept as previously mentioned. This remark highlights the necessity of first establishing legal guidelines for determining whether a conduct qualifies as one that carries criminal penalties (Sri Rahayu, 2014).

When dealing with cybercrime in practice, the notion of legality is analogous to tackling the difficulty of normative gaps in the Criminal Code (KUHP). The Criminal Code (KUHP) was drafted during the Dutch colonial era and did not recognize technology-related offenses like as hacking, digital data manipulation, or virus propagation. As a result, law enforcement must follow certain restrictions, such as the Electronic Information and Transactions Law (ITE).

The main legislative foundation for preventing cybercrime is the Electronic Information and Transactions Law (ITE). But as it turns out, certain of the ITE Law's provisions—like Article 27 paragraph (3) on defamation—are viewed as ambiguous and vulnerable to abuse (Wahyuni, 2020). In this scenario, law enforcement frequently employs the principle of analogy, which directly opposes the idea of legality. To handle forms of cybercrime that have not been formally regulated, some investigators and prosecutors employ teleological or systematic interpretation. Several court cases demonstrate different interpretations of the ITE Law's articles.

The 2019 elections provide as a real-world example, since a Distributed Denial of Service (DDoS) attack on the official KPU website disrupted public access to election result information. It is believed that domestic parties were involved in this attack, which started from foreign IP addresses. However, there are a number of obstacles that law enforcement must overcome to combat the criminals (Putra, 2024).

According to the author, people can only be punished for acts that have been expressly classified as crimes under earlier laws, as per the legality principle (nullum crimen sans lege, nulla poena sine lege). Despite obvious intent (mens rea) and wrongdoing (actus reus), law enforcement authorities have trouble enforcing punishments since "DDoS" is not well defined. In this regard, the author contends that criminal law theory is ineffective as a framework for dealing with crimes involving technology. In order to be more sensitive to the evolution of digital crime forms without compromising the ideals of the rule of law, it is imperative that the legality concept be rethought.

The social construction of crime and criminality, which are the focus of criminology and criminal justice studies, contrasts with the production of crime (criminal law). I will first examine two facets of the contemporary legal construction of crime, with a particular focus on criminal law: its conceptual shape and its substantive extent. I will also situate this research in a historical and social framework, describing the connection between criminal law and criminological/penal studies as well as between the law and the social production of crime (Lacely, 2012).

Modern criminal law literature proposes the reform of offenses by considering several elements, namely the element of cyber mens rea or intent in the context of technology use, the element of digital actus reus or digital actions such as unauthorized system access, and non-physical consequences as a form of harm recognized in criminal law (Hamzah, 2017).

In actuality, crimes like phishing, sniffing, DDoS, and ransomware which are not expressly listed as crimes in the Penal Code or the ITE Law are not directly mentioned in criminal law rules. While cybercrime can involve a click, script insertion, or manipulation, criminal law offenses are solely dependent on the conventional understanding of acts as physical activities. Furthermore, many commonplace cybercrimes are not recognized as illegal activities because the criteria of criminal law are vague.

As demonstrated by the instance in Indonesia, on June 20, 2024, an unidentified gang entered the National Data Center (PDN) and launched a ransomware attack, resulting in one of the biggest cyberattacks in Indonesian history. Over 282 government agencies, including ministries, organizations, and local governments, were among the impacted systems. Several state agencies, including immigration, were rendered fully inoperable for several days as a result of this attack, and the attackers wanted a ransom of up to US$8 million (about Rp131 billion). However, no serious judicial action has been taken against the offenders several months after the incident (Jatmiko, 2024). According to the author, the example shows that these kinds of instances might happen not just because it can be challenging to find transnational criminals but also because neither the Criminal Code nor the ITE Law explicitly address such crimes.

Thirdly, criminal liability is basically a mechanism created by criminal law to address agreements to abstain from particular behaviors (Candra, 2013). In practice, the discrepancy between this theory and cybercrime is caused by the ambiguous concept of corporate digital responsibility, the difficulties in establishing the element of Mens Rea, and the hazy identity of the offender (Wibowo, Muhammad Singgih Imam, Munawar, Akhmad, 2024).

It seems that the idea of criminal culpability has not adequately addressed cybercrime in the context of law enforcement's actions in the Bjorka case. Despite the fact that numerous significant pieces of information, such as SIM registrations (1.3 billion data), internal BIN documents, and BSSN archives, have been publicly published on BreachForums and Telegram, the perpetrator's identity is still unknown (Prasasti, 2022).

The aforementioned case demonstrates that the vague identity of the offender, the difficulty in establishing the suspect's mens rea, and the lack of a digital corporate entity being held accountable are the main reasons why the theory of criminal liability is ineffective in the practice of law enforcement regarding cybercrime.

Based on the aforementioned data, the author draws the conclusion that the theory of criminal law as a body of legal literature is inefficient when compared to Indonesian law enforcement's cybercrime enforcement techniques. This indicates that in the digital age, criminal law theories continue to fall short of providing a legal framework for addressing cybercrime-related problems.

Therefore, a revival of the idea of criminal law that is not just normative but also sensitive to the intricate, global, and decentralized nature of cybercrime is necessary in order to achieve a fundamental alignment between theory and practice. The criminal culpability model must be expanded to encompass digital entities and businesses, the legality principle must be reconstructed to be more responsive to new forms of crime, and the technologically supported evidential system must be strengthened. Criminal law will continue to be reactive and fall behind in tackling the more intricate and extensive problems associated with cybercrime in the absence of these sophisticated conceptual approaches.

According to the research's findings, law enforcement needs to improve their knowledge and proficiency with the constantly changing categories of cybercrime, particularly with regard to digital forensics, data-based evidence, and identifying offenders in different countries. To handle operating modes that are no longer physical or individual, legal practices that still rely on traditional tools and techniques must be altered right away.

This study offers a chance for criminal law theory to be reconstructed in an academic setting that is more compatible with the digital era. Fundamentally, this writing policy will support the development of more flexible and progressive criminal law regulations, such as the modification or establishment of new standards outside of the Criminal Code and the ITE Law that are better suited to the digital world. In order for Indonesia to become both a target of cybercrime and an active and sovereign legal subject, the government and lawmakers must think about creating a distinct cyber law code that combines aspects of criminal law, digital forensics, cybersecurity, and international jurisdiction.

CONCLUSION

This study demonstrates that Indonesia is still making progress toward a more thorough understanding of the development of criminal law concepts in response to cybercrime. The literature has not yet been able to adequately address types of cybercrime that are digital, decentralized, and anonymous because it still tends to be based on traditional offenses included in the Criminal Code. There hasn't been a harmonic match between criminal law theory and law enforcement's approach to combating cybercrime thus far. Due to inadequate legislation and a lack of technological resources, law enforcement officials frequently encounter challenges in demonstrating components of guilt, criminal culpability, and the fulfillment of the legality principle in practice.

Consequently, it may be said that the degree to which Indonesia's cybercrime laws can be successfully enforced in the digital age depends heavily on the success or efficacy of criminal theory in criminal law literature. As a result, it becomes crucial to link theory and practice when developing structural and paradigmatic legal reform initiatives as well as at the normative level. According to this study, Indonesia will continue to have a difficult time successfully enforcing the law against increasingly sophisticated and pervasive cybercrime until criminal law theory is updated to be more suited to the digital environment.

REFERENCES

Aini, N., & Lubis, F. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. *Judge: Jurnal Hukum*, *05*(02), 55–63. http://www.journal.cattleyadf.org/index.php/Judge/article/view/566%0Ahttp://www.journal.cattleyadf.org/index.php/Judge/article/download/566/433

Aldriano, M. A., & Priyambodo, M. A. (2022). Cyber Crime Dalam Sudut Pandang Hukum Pidana. *Jurnal Kewarganegaraan*, *6*(1), 2169–2175.

Basreskrim Polri. (2025). *Jumlah Laporan Polisis Yang Dibuat Masyarakat*. Patroli Siber. https://patrolisiber.id/statistic/

Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia. *Refleksi Hukum: Jurnal Ilmu Hukum*, *3*(2), 145–160. https://doi.org/10.24246/jrh.2019.v3.i2.p145-160

Candra, S. (2013). Konsep Pertanggungjawaban Pidana Nasional Yang Akan Datang. *Jurnal Cita Hukum*, *1*(1), 19.

Ginara, I. G. K., Widyantara, I. M. M., & Styawati, N. K. A. (2022). Kriminalisasi Terhadap Kejahatan Carding Sebagai Bentuk Cyber Crime dalam Hukum Pidana Indonesia. *Jurnal Preferensi*

Hukum, *3*(1), 138–142. https://doi.org/10.22225/jph.3.1.4673.138-142
Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, *23*(2), 400–426. https://doi.org/10.15642/alqanun.2020.23.2.400-426
Hamzah, A. (2017). *Delik-Delik Khusus: Tindak Pidana di Bidang Teknologi Informasi*. Sinar Grafika.
Jatmiko, L. D. (2024). *Pemerintah Diminta Kejar Aktor Kejahatan Siber, Beri Sanksi Hukum*. Tekno. https://teknologi.bisnis.com/read/20240125/84/1735521/pemerintah-diminta-kejar-aktor-kejahatan-siber-beri-sanksi-hukum?utm_source=chatgpt.com
Kominfo. (2024). *Laporan Tahunna Keamanan Siber Nasional 2024*. Kementerian Komunikasi dan Informatika.
Lacely, N. (2012). Legal Constructions Of Crime. *Academia Edu*. https://doi.org/https://doi.org/10.1093/HE/9780199590278.003.0006
Mewengkang, I. B., Warong, R. N., & Kuntag, M. (2021). Kajian Yuridis Cyber Crime Penanggulangan Dan Penegakan Hukumnya. *Lex Crimen*, *10*(5), 26–35.
O.S, E. (2020). *Asas Legalitas dan Penafsiran dalam Hukum Pidana*. Cahaya Atma Pustaka.
Prasasti, G. D. (2022). *Ramai Aksi Bjorka Bocorkan Data, BSSN Angkat Bicara*. Liputan 6. Dalam praktik penegakan hukum terhadap kasus Bjorka, terlihat bahwa teori pertanggungjawaban pidana belum efektif menjangkau kejahatan siber. Identitas pelaku tetap kabur walaupun berbagai data penting telah dibocorkan secara terang-terangan di BreachForums dan Telegram, termasuk registrasi SIM (1,3 miliar data), dokumen internal BIN, dan arsip BSSN
Putra, H. R. (2024). *KPU Sebut Adanya Gangguan DDoS pada Sirekap sejak Hari Pemungutan Suara*. Tempo. https://www.tempo.co/politik/kpu-sebut-adanya-gangguan-ddos-pada-sirekap-sejak-hari-pemungutan-suara-85560
Salsabilla, A., & Angelina, J. (2024). *Peran Hukum Pidana Dalam Menangani Kejahatan Siber pada Masa Sekarang : Tinjauan Terhadap Undang Undang Informasi Transaksi Elektronik*. *2*(2), 1548–1554.
Sofian, A. (2021). Dilema Penegakan Hukum Terhadap Kejahatan Siber: Studi atas Proses Pembuktian Digital. *Jurnal Hukum & Teknologi*, *3*(2), 113–115.
Sri Rahayu. (2014). Implikasi Asas Legalitas Terhadap Penegakan Hukum dan Keadilan. *Jurnal Inovatif*, *VII*(September), 4. https://online-journal.unja.ac.id/jimih/article/view/2170
Sugiaryo. (2010). KEBIJAKAN REGULASI HUKUM PIDANA DALAM MENANGANI KEJAHATAN TEKNOLOGI INFORMASI Oleh : Sugiaryo (Staf Pengajar UNISRI Surakarta). *Jurnal Serambi Hukum*, *04*(02).
Supriyadi, S. (2017). Community of Practitioners: Solusi Alternatif Berbagi Pengetahuan antar Pustakawan. *Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi Dan Kearsipan*, *2*(2), 83. https://doi.org/10.14710/lenpust.v2i2.13476
Syahrir, M., Tunggal, U. T., Surabaya, K., Timur, J., Pekerjaan, A., Kupang, S., Kupang, K., Timur, N. T., Info, A., Enforcement, L., Prevention, C., & Law, C. (2025). *Efektivitas Hukuman bagi Pelaku Kejahatan Siber di Indonesia: Analisis Kriminologi dengan Metode Content Analysis*. *3*(1), 694–711. https://doi.org/10.51903/perkara.v3i1.2343
Wahyuni, S. (2020). Penafsiran Hukum terhadap Pasal 27 ayat (3) UU ITE dan Ancaman Kebebasan Berekspresi. *Jurnal Hukum & Teknologi*, *5*(1), 23.
Wibowo, Muhammad Singgih Imam, Munawar, Akhmad, dan H. (2024). KENDALA TEKNIS DAN HUKUM DALAM PROSES PENYIDIKAN TINDAK PIDANA SIBER DI INDONESIA TECHNICAL AND LEGAL OBSTACLES IN THE INVESTIGATION PROCESS OF CYBER CRIMES IN INDONESIA. *Jurnal Hukum Lex Generalis*, *5*(7). https://ojs.rewangrencang.com/index.php/JHLG/article/view/641/280