GIJLSS
Greenation International Journal of Law and Social Sciences
+62 81210467572 https://research.e-greenation.org/GIJLSS greenation.info@gmail.com
GREENATION RESEARCH

DOI: https://doi.org/10.38035/gijlss.v3i3

Transforming Cybercriminal Law Governance through an Interdisciplinary Approach as an Effort to Achieve Global Prosperity

Amalia Sari[1], KMS Herman[2]
[1]Universitas Borobudur, Jakarta, Indonesia, ziaamel86@gmail.com
[2]Universitas Borobudur, Jakarta, Indonesia, kms_herman@borobudur.ac.id

Corresponding Author: ziaamel86@gmail.com@gmail.com[1]

Abstract: The development of information technology in the digital era has given rise to various forms of cybercrime that are cross-border and have a significant impact on legal, social, and economic aspects. The complexity of cybercrime poses challenges for national criminal laws that are often lagging behind technological dynamics. This condition not only threatens legal certainty and the protection of people's rights, but also has an impact on the stability of the digital economy, data security, and social justice. To analyze the extent to which criminal law regulation in Indonesia has been able to answer the complexity of cross-border cybercrime and to formulate a concept of transforming cyber-criminal law governance that is more adaptive, responsive, and oriented towards global welfare. The method used is normative juridically, using a legislative approach and an analytical approach. Research shows that the weaknesses of cyber-criminal law in Indonesia lie in the disharmonization of regulations, the limited capacity of law enforcement officials, the lack of use of digital forensic technology, and the weak cooperation across countries. Governance transformation can be realized through regulatory harmonization, increasing digital literacy of law enforcement officials, applying technology in proof, and strengthening international cooperation mechanisms. In conclusion, the governance of cyber-criminal law based on an interdisciplinary approach not only provides legal certainty and protection for the community, but also contributes to the creation of global prosperity in the digital era.

Keywords: Cybercrime Law, Governance Transformation, Interdisciplinary Synergy, Global Well-Being

INTRODUCTION

The development of information and communication technology in the digital era has fundamentally altered the global social, economic and political landscape. While this transformation has had a positive impact on the efficiency, connectivity and progress of the digital economy, it has also given rise to serious challenges in the form of increasing cross-border, multidimensional cybercrime. Ransomware, personal data theft, online fraud and the

misuse of artificial intelligence are all real threats to legal stability, national security and social justice. Not only does cybercrime threaten the right to privacy and data protection, it also disrupts the digital economy and undermines people's trust in secure cyberspace.

Very rapid technological developments also necessitate adjustments to regulations and legal policies that are more adaptive and responsive to the dynamics of the digital world. Given its cross-border nature and the fact that it is difficult to control by a single jurisdiction, countries around the world must work together to build a strong international framework to effectively prevent and tackle cybercrime. Increasing digital literacy and public awareness of cybersecurity is also important in strengthening defenses against increasingly sophisticated cyber threats.

Cybercrime or cybercrime is defined as a criminal act committed using computer technology as the main crime tool. This crime takes advantage of the development of computer technology, especially the internet (Marita, 2015). Cybercrime is a criminal act that has several characteristics. These crimes include unauthorized access aimed at facilitating crime. In addition, this action also includes unauthorized alteration or destruction of data, as well as interfering with or damaging computer operations. Last but not least, cybercrime can also include actions that prevent or hinder access to computers. These characteristics show how complex and diverse the forms of cybercrime are today (Tobing et al., 2024).

Changes in the global digital landscape require a transformation of cyber-criminal law governance that does not only focus on enforcement aspects (*repressive function*), but also on aspects of prevention, adaptation, and collaboration across disciplines (Cahyono et al., 2025). An interdisciplinary approach is the main key in the transformation process. The law cannot stand alone to answer the complexity of the cyber world involving technical, social, and psychological aspects. In the Indonesian context, the criminal law system is still trying to catch up with the rapid development of information technology. Existing legal instruments such as the Criminal Code (KUHP), Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, and various sectoral regulations have not been fully able to accommodate the complexity and transnational character of cybercrime. These limitations create an urgent need to transform the governance of cyber criminal law that is oriented towards inter-disciplinary synergy and cross-sector harmonization.

The transformation of cyber-criminal law governance must also be directed to ensure global welfare as the ultimate goal. Digital security is no longer just a matter of national law, but part of the world's welfare system (Wibowo, 2023). A safe and fair cyberspace creates public trust in digital transactions, supports global economic growth, and strengthens the protection of human rights in the technological age (Najwa, 2024). Thus, cybercriminal law not only serves to protect against crime, but also to build the foundation for social justice and equitable prosperity at the international level.

In this context, the law must be transformed from just a control tool to an instrument of governance that is able to balance between freedom and digital security (Azura et al., 2022). Good cyber criminal law not only cracks down on perpetrators, but also encourages the formation of an ethical, transparent, and sustainable digital ecosystem. This requires harmonious regulatory reforms, strengthening the capacity of law enforcement officials through digital literacy, and increasing international cooperation in tackling cross-border cybercrime.

The novelty of this research lies in the integration between criminal law, information technology, and global governance in building a new paradigm of cyber criminal law in Indonesia. Unlike previous research that placed law and technology separately, this study confirms that the sustainability of digital justice can only be achieved through

interdisciplinary collaboration that balances legal certainty (*rechtszekerheid*), technological advancement, and human rights protection.

Using normative juridical methods and international analysis and comparison approaches, this study aims to: (1) analyze the extent to which criminal law in Indonesia has been able to answer the complexity of cross-border cybercrime; and (2) formulate a concept of cyber-criminal law governance transformation based on an interdisciplinary approach and oriented towards global welfare.

Therefore, this research not only makes a theoretical contribution to the development of modern criminal law in the digital era, but also offers a practical foundation for policymakers and law enforcement officials to build fair, safe, and sustainable cyber governance as part of Indonesia's commitment to realizing global prosperity amid the challenges of the digital revolution.

METHOD

The approach method used is normative juridical research. The normative juridical research method is a literature law research conducted by examining literature materials or secondary data. (Sedarmayanti & Hidayat, 2011). Normative juridical research is a process to find legal rules, legal principles, and legal doctrines to answer the legal problems faced. (Marzuki, 2019). The instruments in this study consist of literature review and analysis of legal documents. (Soekanto & Mahmudji, 2003).

The objects of the research include national regulations of the Criminal Code (KUHP), Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions. The data used is secondary data, including primary legal materials, namely related laws and regulations, secondary legal materials in the form of books, journals and related literature, and tertiary legal materials, namely dictionaries and legal encyclopedias.

Data collection was carried out through literature studies, while data analysis used qualitative-descriptive analysis. This research is limited to normative and conceptual studies without empirical data collection, but provides a theoretical contribution in formulating a model of cyber-criminal law governance transformation that is interdisciplinary, adaptive, and oriented towards global welfare.

RESULT AND DISCUSSION

1. Indonesia's Criminal Law Regulation Capacity in Responding to the Complexity of Cross-Border Cybercrime

The development of information and communication technology (ICT) in the 21st century has transformed almost every aspect of human life, including economic activities, government and education, as well as social relations. This marks a significant transition from an industrial to an information society, where data and digital technology are the primary sources of economic and social power. In the economic sphere, ICT has enabled new business models to emerge, such as e-commerce, fintech and digital platforms that connect producers and consumers more efficiently, transcending geographical boundaries. In government, digitalization is encouraging the delivery of more transparent, efficient and accountable public services through e-government and smart cities. In education, meanwhile, access to digital learning resources and distance learning technology opens up wider opportunities for people to acquire knowledge in an inclusive and flexible manner. In the social realm, interaction and communication between individuals has become more dynamic and complex through social media and instant messaging applications. However, this also poses new challenges, such as the spread of misinformation and social polarization. Overall, this advance in ICT has changed not only the way humans operate, but also shifted the

paradigm of modern life towards an era that is increasingly connected and dependent on digital technology. Various innovations such as artificial intelligence blockchain and cloud computing has created incredible efficiencies in various areas of life (Oktareza et al., 2024). However, behind this progress that brings great benefits to the well-being of humanity, there are also new forms of crime that are complex, sophisticated, and difficult to trace, known as cybercrime (Febriansyah, 2025).

Cybercrime has unique characteristics because it knows no geographical boundaries, is carried out with digital devices, and is often anonymous and cross-jurisdictional (Yusni et al., 2025). The perpetrator can be in one country, the victim in another, while the server or infrastructure used is in a third country. This complexity poses a serious challenge to the national criminal law system which is still basically based on the classic principle of territoriality, namely that criminal law only applies to acts committed within the territory of the state. As a result, the fundamental question arises about who has the authority to adjudicate, where *locus delicti* a crime is considered to have occurred, and how electronic evidence can be assessed as valid evidence in court (Simada et al., 2024).

In the context of Indonesian law, this issue is even more complicated because the existing legal apparatus is not fully able to accommodate the character of this borderless digital crime (Paradise, 2024). The conventional legal system tends to be oriented towards the physical aspect of a criminal act, while the cyber world is virtual and distributed. This condition shows that there is a normative gap between the reality of modern crime and the criminal law structure that is still tied to the old paradigm. Therefore, it is necessary to reform and transform the governance of cyber criminal law that not only upholds justice in the national realm, but is also able to respond to global challenges with an interdisciplinary approach that integrates digital law, technology, and ethics in a balanced manner.

a. Substance Limitations and Regulatory Fragmentation

National legal instruments that are the basis for countering cybercrime in Indonesia include the Criminal Code (KUHP), Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, **Law Number 27 of 2022 concerning Personal Data Protection, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions**, as well as various other sectoral regulations governing digital security, electronic transactions, and digital consumer protection.

From perspective **Integration and effectiveness**, these regulations have not yet established a comprehensive cyber criminal law system. Exist **Vertical and horizontal disharmonization**, where definitions, scopes, and sanctions between regulations often overlap. As a result, legal uncertainty arises (*legal uncertainty*) in enforcement practice. Many cybercrime cases are difficult to process due to differences in interpretations between law enforcement agencies, such as the police, prosecutor's office, and Kominfo. This disharmony is also seen in non-uniform court rulings, where judges often interpret the elements of "disenfranchised" or "unlawful" narrowly, so that many cybercriminals escape the snare of the law (Cahyono et al., 2025).

b. Law Enforcement Aspects and Apparatus Capacity Limitations

Law enforcement against cybercrime in Indonesia still faces various serious obstacles, both in terms of human resources, infrastructure, and institutional coordination. Although regulations have been made available through their implementation, they have not been effective because the ability of law enforcement officials is still limited in understanding and handling complex and cross-border digital crimes.

Most of the apparatus does not have adequate digital forensic competence, making it difficult to analyze and verify *digital evidence* in the investigation and court evidence process. The limited forensic laboratory facilities and supporting equipment at the regional level cause the investigation process to often depend on the center and run slowly. This condition is exacerbated by weak coordination between institutions such as the National Police, BSSN, Communication and Informatics, and the Prosecutor's Office which are still working sectorally without an integrated system.

Law enforcement infrastructure is also not in line with technological developments, while criminals are taking advantage of encryption technology and anonymous networks that are difficult to track (Judianto, 2025). As a result, many cyber cases are not resolved or are delayed in legal proceedings. This condition shows that the main weakness of cyber criminal law in Indonesia lies not in the substance of the regulation, but in its law enforcement capacity. Therefore, improving the technical capabilities of the apparatus, strengthening digital forensic laboratories, and establishing a national coordination mechanism are urgent steps so that cyber criminal law can be enforced effectively, quickly, and fairly in the digital era.

c. Jurisdictional Challenges and International Cooperation

Obstacles to jurisdiction and international cooperation are the main obstacles in enforcing cyber-criminal law in Indonesia. The borderless character of cybercrime , namely the perpetrators, victims, and servers can be in different countries, raises a fundamental question: which country has the authority to investigate, prosecute, and prosecute? Indonesia's legal system, which still uses classical territorial principles (applicable to acts within sovereign territory) is often inadequate for cross-border cases.

In practice, most countries have different regulations and judicial systems, so the procedural requirements are not aligned. Cyberattacks are often hidden and involve actors who are difficult to track because they are outside national jurisdiction so The inconsistency of standards and procedures between countries causes obstacles in the effective application of international law (Susilowati, 2025).

The problem is even more complex because Indonesia has not ratified the Budapest Convention on Cybercrime (*Budapest Convention on Cybercrime*), which is the main instrument in encouraging harmonization of norms and cross-border legal cooperation (Febrian et al., 2024). Indonesia's non-involvement in the convention is an obstacle for the country to maximize international cooperation, such as the exchange of electronic evidence data and the provision of legal aid between countries.

2. The Concept of Transforming Cybercriminal Law Governance that is Adaptive, Responsive, and Oriented to Global Welfare

The transformation of cyber criminal law governance is an inevitable necessity in the midst of information technology advances that have penetrated national borders and changed the face of crime in the digital era. Cybercrime is now more complex and dynamic, involving various modus operandi that are difficult to anticipate with conventional legal frameworks that are often still rigid and territorial. In the global context, cybercrime is no longer local or conventional, but involves cross-border networks, the use of advanced technologies, and complex and ever-evolving modes (Pramudya & Yusuf, 2025). This situation demands a fundamental update to the national criminal law paradigm to be more adaptive to technological changes, more responsive to social and law enforcement needs, and oriented towards global welfare as a form of state responsibility for digital security and justice.

Conceptually, the transformation of cyber criminal law governance means a shift from a reactive and sectoral legal system to a legal system that is integrative, collaborative, and based on multidisciplinary knowledge. Law is no longer understood solely as a rigid normative device, but as a living and dynamic system, which must be able to adapt to social and technological changes (Sainul et al., 2024). A legal approach that focuses only on regulatory texts is no longer adequate in dealing with cybercrime based on interconnected algorithms, data, and digital systems. In this case, criminal law needs to be transformed into a governance instrument (*governance instrument*) that is able to strike a balance between legal protection, digital security, and freedom of expression in cyberspace (Abdurrohman et al., 2025).

Adaptive cyber criminal law demands legal updates that are relevant to technological advances and the conditions of the digital society. Regulations regarding cybercrime must be formulated precisely in order to reach various new forms of crime such as personal data theft, artificial intelligence manipulation (*AI manipulation*), *ransomware*, and digital financial crimes. Legal norms must be constructed by paying attention to the characteristics of the cyber world that are infinite and without physical form. In this context, criminal law must accommodate the concept of extraterritorial jurisdiction, as applied in the *Budapest Convention on Cybercrime*, so that the state can still enforce the law against cybercrime perpetrators even if the perpetrators are outside the sovereign territory. Adaptivity also includes strengthening the digital evidence aspect, where the criminal justice system needs to recognize the validity of electronic evidence and apply technology-based evidentiary standards such as *the digital chain of custody* and *blockchain verification system* to ensure the integrity of evidence in legal proceedings.

More than just a revision of regulations, the adaptability of cyber criminal law also means a change in the perspective of the law itself. The law should not be static, but must be able to predict the direction of technological development so that it is not always left behind by digital innovation. A predictive approach in law allows policymakers to formulate norms that are anticipatory, not just reactive. For example, arrangements regarding the use of artificial intelligence, biometric data protection, and digital platform responsibilities need to be designed with the principles of prudence and risk-based. Thus, criminal law no longer functions only as a punishment mechanism, but also as a system of protection and prevention in a digital society.

Responsive cybercriminal law emphasizes the ability of legal systems to adapt to social and institutional needs in the face of digital crime threats. Responsiveness means that the law does not run alone, but moves through synergy between actors: the state, law enforcement agencies, academics, the private sector, and civil society (Rok Su, 2024). In the Indonesian context, this includes improving institutional governance so that there is no overlap of authority between the police, prosecutor's office, BSSN, Kominfo, and other institutions involved in handling cybercrime. An integrated coordination system is needed through institutions that have a national mandate to coordinate policies, investigations, and evidence in cyber cases. With strong institutional governance, the law enforcement process will be more efficient, directed, and free from sectoral egos that have been the main obstacles.

The responsiveness of cyber criminal law is also realized through increasing the capacity of law enforcement human resources to have digital competence. Law enforcement officials need to understand the basic principles of digital forensics, data analysis, cyber trail tracking, and the use of artificial intelligence technology to detect crimes in cyberspace. In addition, synergy between law enforcement agencies and universities must be strengthened so that academic research can contribute directly to technology-based law enforcement innovation. In this perspective, responsive cybercriminal law is not only oriented towards the

speed of enforcement, but also on accuracy, reliability, and adaptability to evolving crime patterns.

The concept of transforming cyber criminal law governance cannot be separated from its orientation towards global welfare. Good law not only guarantees security, but also creates justice and prosperity for the wider community (Butarbutar et al., 2025). In the global digital ecosystem, cybersecurity is the main foundation for economic growth and the welfare of the world's people. Trust in digital systems, data stability, and protection of individual privacy are important prerequisites for the development of an inclusive and sustainable digital economy. Therefore, effective cybercriminal law governance directly contributes to economic stability, social security, and improving people's quality of life.

In the framework of development law (*law as a tool of social engineering*), cyber criminal law must be a means of social engineering to create a safe and ethical digital ecosystem. A law that is oriented towards global well-being means a law that is able to protect society from the threat of digital crime while encouraging equitable economic participation in cyberspace. With clear regulations, strong legal protection, and transparent law enforcement, people will have more trust in digital systems. This trust is an important social capital in strengthening the transformation of the national and global digital economy.

Global well-being is also related to human values and digital justice (*digital justice*). From a human rights perspective, access to digital security, personal data protection, and freedom of expression are fundamental rights that must be guaranteed by the state. Therefore, the transformation of cyber criminal law must contain humanistic values that respect human dignity in the midst of technological advances. The state is not only responsible for cracking down on criminals, but also ensuring that regulations are not used arbitrarily that can limit citizens' rights in the digital space (Nainggolan et al., 2024).

In the end, the concept of transforming cyber criminal law governance that is adaptive, responsive, and oriented towards global welfare emphasizes the need for an interdisciplinary approach in formulating and implementing criminal law in the digital era. Law must combine with science, technology, public policy, digital economy, and social ethics in order to be able to build a progressive and fair legal system. Adaptive law provides a foundation of certainty; responsive laws ensure efficiency and collaboration; And global well-being-oriented laws ensure that digital justice is enjoyed not only by a small segment of society, but by the entire human race. Thus, the transformation of cyber criminal law governance is not just a change in regulations, but a paradigm shift towards a more inclusive, fair, and global benefit-oriented legal order.

CONCLUSION

This research shows that Indonesia's capacity for dealing with cross-border cybercrime under criminal law is still limited, and has not fully adapted to the rapid and dynamic development of information technology. The main obstacles to enforcing the law in cyberspace are regulatory fragmentation, disharmonisation between regulations, and law enforcement officials' limited understanding of the characteristics of digital crime. A national legal system based on traditional territorial principles is inadequate for addressing the complexities of borderless cybercrime. Additionally, Indonesia's cyber-criminal law enforcement is often hampered by differences in jurisdiction and legal standards between countries due to the lack of ratification of the Budapest Convention on Cybercrime and weak international cooperation.

The results of this study are important because they emphasise the need for cyber-criminal law reform to transform legal governance into something that is adaptive, responsive and oriented towards global welfare. Adaptability is required to enable the law to keep pace with technological developments, accommodate digital evidence, and address cross-border

jurisdictions. Responsiveness requires institutional strengthening, capacity building of human resources, and cross-sectoral collaboration to confront ever-evolving criminal modes. Meanwhile, an orientation towards global welfare establishes the law as a means of protecting digital human rights, social justice and economic security in the digital transformation era.

Thus, the results of this study confirm that cyber-criminal law cannot be understood as merely a law enforcement instrument; it must also be part of a global governance system that ensures digital justice and security for all of humanity. Reforms based on the synergy between law, technology and digital ethics would strengthen Indonesia's role in the global cybersecurity system and encourage the creation of an inclusive and equitable digital economy.

REFERENCES

Abdurrohman, A. H., Uzmawi, C. N., Khoiruddin, R., & Mustain, A. M. (2025). *Cybersecurity dan Pancasila : Harmonisasi Regulasi Hukum Internasional dengan Kepentingan Nasional*. *1*(March), 23–29.

Azura, R., Rofinda, Z. D., Rusjdi, S. R., Husni, Mahata, L. E., & Fadila, Z. (2022). Jurnal Riset Ilmiah. *Jurnal Riset Ilmiah*, *1*(01), 15–18. https://manggalajournal.org/index.php/SINERGI/article/view/1218/1479

Butarbutar, A. S., Butarbutar, E. N., Studi, P., Program, H., Universitas, M., & Saanto, K. (2025). *Peran hukum dalam mewujudkan negara kesejateraan republik indonesia yang berkeadilan sosial*. *2*(2), 123–133.

Cahyono, S. T., Erni, W., & Hidayat, T. (2025). Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia. *Dame Journal of Law*, *1*(1).

Febrian, W. R., Faturrahman, R. M. R., Rahmadina, H. S., & Deni, F. (2024). Peran Hukum Internasional Dalam Menangani Kasus Cyber Crime. *Jurnal Sahid Da'Watii*, *3*(02), 1–7. https://doi.org/10.56406/jurnalsahiddawatii.v3i02.481

Febriansyah, F. I. (2025). *Cybercrime Kejahatan di Balik Layar Digital* (1 ed.). Najaha.

Firdaus, R. A. (2024). Perlindungan Hukum dan Pencegahan Kejahatan Siber di Era Digital dalam Sistem Hukum di Indonesia. *Jurnal Hukum Kenegaraan dan Politik Islam*, *4*(1).

Judijanto, L. (2025). Hukum Pidana dan Kejahatan Siber: Menanggulangi Ancaman Kejahatan Digital di Era Teknologi. *Indonesian Research Journal on Education*, *5*(1), 1079–1085.

Marita, L. S. (2015). Cyber Crime Dan Penerapan Cyber Law Dalam Pemberantasan Cyber Law Di Indonesia. *Cakrawala:Jurnal Humaniora Unievrsitas Bina Sarana Informatika*, *15*(2).

Marzuki, P. M. (2019). *Penelitian Hukum Edisi Revisi*. Kencana.

Nainggolan, A., Lumbantoruan, I. E., & Manalu, S. (2024). Eksistensi Negara Hukum Dalam Era Digital. *Mimbar Keadilan*, *6*(2), 62–70.

Najwa, F. R. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dah Hukum*, *2*(1), 8–16. http://ejournal.unisi.ac.id/index.php/albahts/article/view/3044%0Ahttp://ejournal.unisi.ac.id/index.php/albahts/article/download/3044/1574

Oktareza, D., Noor, A., Saputra, E., & ... (2024). Transformasi Digital 4.0: Inovasi yang Menggerakkan Perubahan Global. *Jurnal Hukum, Sosial*, *2*(3), 661–672. https://journal.lps2h.com/cendekia/article/view/98%0Ahttps://journal.lps2h.com/cendekia/article/download/98/78

Pramudya, D. W., & Yusuf, H. (2025). PENANGGULANGANNYA DARI PERSPEKTIF KRIMINOLOGI ANATOMY OF CYBER CRIME : MOTIVES , MODES , AND COUNTERMEASURES FROM A CRIMINOLOGICAL PERSPECTIVE. *Jurnal Intelek Insan Cendikia*, *2*(8), 14613–14623.

Rok Su, B. (2024). Dari Teori Ke Praktik: Strategi Responsivitas Hukum Terhadap Tantangan Ekonomi Dan Sosial From Theory To Practice: Legal Responsiveness Strategies To Economic and Social Challenges. *Jurnal Hukum Lex Generalis*, *5*(10), 1–20. https://jhlg.rewangrencang.com/

Sainul, Oktavia, A., & Angkasa, N. (2024). Hubungan Perubahan Sosial dan Perubahan Hukum Dalam Sistem Hukum Terbuka. *Siyasah Jurnal Hukum Tatanegara*, *4*(2), 123–136. https://doi.org/10.32332/w0wsa066

Sedarmayanti, & Hidayat, S. (2011). *Metodologi Penelitian*. Mandar Maju.

Simada, A., Kalo, S., Ekaputra, M., & Leviza, J. (2024). Penentuan Locus Delictie dalam Tindak Pidana Cyber Crime (Merusak dan Mengganggu Sistem Elektronik dan Komunikasi Milik Orang Lain). *Locus Journal of Academic Literature Review*, *3*(4), 349–361. https://doi.org/10.56128/ljoalr.v3i4.314

Soekanto, S., & Mahmudji, S. (2003). *Penelitian Hukum Normatif*. Raja Grafindo Persada.

Susilowati, A. (2025). Penegakan Hukum Internasional terhadap Serangan Siber terhadap Infrastruktur Kritis di Indonesia. *Aliansi: Jurnal Hukum, Pendidikan dan Sosial Humaniora*, *2*(5), 122–141. https://doi.org/10.62383/aliansi.v2i5.1204

Tobing, C. I., Tiofanny Marylin Surya, Selvias, L. R., Stepania Rehulina Girsang, Putri Berliana Azzahra, Lustri Yolanda Purba, Mahezha Agnia Putera, & Nurrahman Rusmana. (2024). Globalisasi Digital Dan Cybercrime: Tantangan Hukum Dalam Menghadapi Kejahatan Siber Lintas Batas. *Jurnal Hukum Sasana*, *10*(2), 105–123. https://doi.org/10.31599/sasana.v10i2.3170

Wibowo, A. (2023). Hukum di Era Globalisasi Digital. *Penerbit Yayasan Prima Agus Teknik*, 192.

Yusni, M., Didik, Hanuring, & Taqyuddin. (2025). *Hukum Siber: Menyikapi Tantangan Hukum di Era Digital*. PT. Nawala Gama Education.