International Journal of Health, Economics, and Social Sciences (IJHESS)
Vol. 7, No. 4, October 2025, pp. 1925~1930
DOI: 10.56338/ijhess.v7i4.8939
Website: https://jurnal.unismuhpalu.ac.id/index.php/IJHESS

Cybercrime and Law Enforcement Challenges in the Era of Criminal Law Digitalization

Juhari[1]*, Sunarto[2], Zabidin[3]
[1-3]Universitas 17 Agustus 1945 Semarang

Article Info

Article history:

Received 30 Sep, 2025
Revised 21 Oct, 2025
Accepted 22 Oct, 2025

Keywords:

Cybercrime, Legal Digitalization, Law Enforcement, Challenges, Regulation

ABSTRACT

The rapid advancement of information technology in the digital era has brought significant convenience to various aspects of human life, yet it has also given rise to new forms of criminal behavior known as cybercrime. This phenomenon encompasses a wide range of unlawful acts such as hacking, data theft, online fraud, and the dissemination of false information, all of which can cause serious social and economic harm. Such developments demand a legal system that can adapt to the dynamic, borderless, and often untraceable nature of cyberspace. This article aims to describe the various types of cybercrimes emerging in Indonesia, analyze the key challenges in law enforcement, and propose strategic measures to strengthen the effectiveness of their handling. The study employs a qualitative method with a normative juridical and descriptive-analytical approach through the examination of relevant literature, legal frameworks, and national research findings. The results indicate that law enforcement against cybercrime in Indonesia faces several obstacles, including regulatory gaps that fail to keep pace with technological progress, limited resources among law enforcement personnel, the complexity of digital evidence, and weak inter-agency and cross-border coordination. Therefore, it is essential to harmonize existing regulations, enhance the technical capacity of law enforcement officers, foster effective international cooperation, and promote public education on digital security to ensure that the national criminal justice system can respond comprehensively and adaptively to the challenges of digitalization.

Corresponding Author:
Juhari
Universitas 17 Agustus 1945 Semarang
*Corresponding Author: Email: juharish.mhum@gmail.com

INTRODUCTION

The rapid advancement of information and communication technology has profoundly transformed nearly every aspect of modern human life. The digital revolution marked by the emergence of the internet, smart devices, and data-driven systems has simplified communication, economic transactions, education, and even governance. Today, most social and economic activities rely heavily on a global and real-time digital network, blurring the traditional boundaries of space and time (Aldriano & Priyambodo, 2022). In this context, technology not only serves as a tool for efficiency but also creates new spaces for deviant behavior and technology-based criminal activities. This phenomenon is known as cybercrime criminal acts committed through computers, networks, or electronic systems as the primary means (Dinda, 2024).

Cybercrime has evolved into a significant threat to national security and the legal system in many countries, including Indonesia. Such crimes not only result in economic losses but also jeopardize data sovereignty, personal security, and social stability (Azzahra, 2025). Unlike traditional crimes, cybercrimes have distinct characteristics they are often anonymous, transnational, and difficult to trace due to the use of digital obfuscation technologies such as Virtual Private Networks (VPNs) and The Onion Router (TOR) (Judijanto & Nugroho, 2025). Moreover, technological innovation frequently outpaces legal adaptation, leading to a regulatory gap between digital realities and existing laws (Hidayat, 2023).

In Indonesia, cybercrime regulation is primarily governed by Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), as amended by Law No. 19 of 2016. This law serves as the main

legal framework for prosecuting crimes committed through electronic systems and the internet. Complementary regulations include Law No. 27 of 2022 on Personal Data Protection (PDP Law), Law No. 1 of 2023 concerning the New Criminal Code (KUHP), and various cyber security directives issued by the National Cyber and Encryption Agency (BSSN). Despite the existence of these legal instruments, law enforcement against cybercrime remains fraught with challenges (Soedirman Law Review, 2023).

A major obstacle lies in the inherent complexity of cybercrime itself. Offenders often operate from outside national jurisdictions, using foreign servers and sophisticated encryption to conceal their identities. This creates difficulties for law enforcement in tracking, gathering, and presenting admissible evidence (Azzahra, 2025). Cybercrimes such as phishing, hacking, scamming, identity theft, and the distribution of illegal content have shown a rising trend in Indonesia. According to BSSN's 2024 report, over 400 million cyberattacks targeted national information systems during the year, with detection success rates remaining below 60% (BSSN, 2024).

Within the realm of criminal law enforcement, evidentiary challenges also persist. Digital evidence central to cybercrime cases differs fundamentally from traditional forms of proof. It is volatile, easily altered or deleted within seconds, and often dispersed across multiple servers worldwide (Aldriano & Priyambodo, 2022). This poses significant difficulties in maintaining the integrity of the chain of custody, an essential component of criminal procedure (Dinda, 2024). Furthermore, limited technical expertise among law enforcement officers in digital forensics frequently hampers investigation and prosecution (Judijanto & Nugroho, 2025).

The issue of human resource capacity is another major concern. Many law enforcement officials including police officers, prosecutors, and judges lack adequate technical knowledge of information technology. Handling cybercrime cases requires advanced understanding of digital security systems, data encryption, and electronic tracing methods. Without these competencies, investigations tend to progress slowly and are prone to technical errors (Hidayat, 2023). Supporting infrastructure, such as digital forensic laboratories, also remains insufficient and unevenly distributed across the country (Soedirman Law Review, 2023).

Indonesia's criminal law is also undergoing a transitional phase with the enactment of Law No. 1 of 2023 on the new Criminal Code (KUHP), which will take full effect in 2026. This new code introduces several provisions addressing technological developments, including offenses involving information systems, communications, and digital data (Hukumonline, 2023). This reflects an awareness of the need for adaptive criminal law that responds to social and technological changes. Nevertheless, debates continue among scholars about whether the new KUHP can adequately accommodate the rapidly evolving nature of cybercrime (Rayyan, 2024).

Cybercrime is not merely a legal issue it is a multidimensional phenomenon encompassing social, economic, political, and national security dimensions. Its impacts extend beyond individuals or corporations, influencing government reputation and public trust in the justice system. When cybercrime cases remain unresolved, public confidence in law enforcement institutions tends to decline (Azzahra, 2025). In the digital economy context, weak legal enforcement against cybercrime can also deter investment and cause significant economic losses (Judijanto & Nugroho, 2025).

Empirical studies indicate that many cybercrime cases fail to reach trial stages due to evidentiary and procedural obstacles. Research by Gadjah Mada University found that only about 40% of reported cybercrime cases proceed to investigation, and merely 20% reach the courtroom (UGM Cybercrime Study, 2023). This highlights the structural and institutional weaknesses of Indonesia's criminal justice system in coping with digital-era crimes. Meaningful reform must therefore go beyond normative adjustments and include substantive and institutional restructuring.

Inter-agency coordination also remains suboptimal. Multiple institutions share overlapping authority in handling cybercrime such as the National Police's Cyber Crime Directorate, BSSN, the Ministry of Communication and Information Technology, and the Financial Services Authority (OJK). The absence of integrated coordination mechanisms has led to fragmented and inefficient enforcement processes (Dinda, 2024). For example, in a 2023 data breach case involving a financial technology application, discrepancies arose between BSSN and the Police regarding jurisdiction and evidentiary standards (Hukumonline, 2023).

Jurisdictional challenges further complicate cybercrime enforcement. These offenses are often cross-border in nature, involving perpetrators, victims, and servers located in different countries. Consequently, national jurisdiction is frequently insufficient to reach offenders abroad. Mutual Legal Assistance (MLA) and extradition processes are time-consuming, depending heavily on international treaties and diplomatic relations (Judijanto & Nugroho, 2025). Since cybercrimes evolve rapidly, delayed responses can result in lost digital evidence and failed prosecutions (Aldriano & Priyambodo, 2022).

In addition to legal and technical barriers, Indonesia's low level of digital literacy exacerbates the cybercrime problem. Many internet users remain unaware of the importance of data protection and digital security. Data from We Are Social (2024) indicate that 78% of Indonesian internet users do not employ two-factor authentication for important accounts, and 62% reuse the same passwords across multiple platforms.

Such behaviors increase vulnerability to data theft, online fraud, and social engineering (Azzahra, 2025).

Poor legal and digital literacy also contributes to the misuse of social media. Many violations of the ITE Law occur simply because users are unaware of legal boundaries in online communication. Cases involving defamation, hate speech, and misinformation are often committed without awareness that these acts constitute criminal offenses (Soedirman Law Review, 2023). Hence, addressing cybercrime in Indonesia requires not only a repressive approach through law enforcement but also preventive strategies emphasizing digital literacy and legal awareness.

The digitalization of criminal law has become inevitable in the modern age. The legal system must evolve to address how digitalization transforms both criminal conduct and legal responses (Hidayat, 2023). Digital legal transformation involves not merely integrating technology into judicial processes but also redefining legal norms, evidence standards, and procedural mechanisms in the context of information technology (Rayyan, 2024). Thus, law enforcement in the digital era must be adaptive, responsive, and grounded in interdisciplinary knowledge combining law, technology, and cybersecurity.

Based on these considerations, the main challenges in enforcing cybercrime laws in Indonesia can be summarized into five key issues: (1) the regulatory lag between technological advancement and legal adaptation; (2) limited technical competence among law enforcement officers; (3) weak inter-agency coordination; (4) jurisdictional barriers in transnational cybercrime cases; and (5) low public awareness of digital security. Unless these problems are addressed, Indonesia's criminal justice system will continue to lag behind the sophistication of modern cyber threats.

Therefore, a comprehensive reform of Indonesia's criminal law system is urgently needed. Such reform should focus not only on legislative updates but also on strengthening institutions, enhancing human resource capacity, and fostering collaboration among government agencies, law enforcement, the private sector, and society. Effective cybercrime enforcement demands a technology-driven and cooperative approach, as well as stronger international engagement. Indonesia should actively participate in global frameworks such as the Budapest Convention on Cybercrime to demonstrate its commitment to combating digital threats (Judijanto & Nugroho, 2025).

Given this background, this article will comprehensively examine the evolving forms of cybercrime in Indonesia, the main challenges faced by law enforcement in the digital era, and strategic policy measures that can enhance the adaptability and effectiveness of the national criminal justice system. This discussion is expected to provide both academic and practical contributions toward strengthening Indonesia's legal response to cybercrime in a fair, efficient, and sustainable manner.

RESEARCH METHOD

This study employs a qualitative research approach with a normative juridical and descriptive-analytical design. This approach is appropriate because the study focuses on examining the legal norms governing cybercrime, the interpretation of statutory provisions, and the analysis of law enforcement challenges in the digital era. The normative juridical method emphasizes the use of primary and secondary legal materials to understand how laws are formulated, applied, and interpreted within the framework of cybercrime enforcement (Marzuki, 2017).

Rather than relying on field data, this research utilizes secondary data obtained through extensive literature review. The review includes books, scholarly articles, legal journals, research reports, and other academic sources discussing cybercrime, legal digitalization, and criminal law enforcement in Indonesia. Primary legal sources analyzed in this study include the Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) and its amendment, Law No. 1 of 2023 on the New Criminal Code (KUHP), Law No. 27 of 2022 on Personal Data Protection (PDP Law), and other derivative regulations addressing cybersecurity and digital law (Soekanto, 2019).

Additionally, data were collected from court rulings, government policies, and official reports issued by state agencies related to cyber law enforcement. Secondary legal materials such as expert opinions, legal doctrines, and academic studies were also examined to strengthen the analysis of Indonesia's evolving cyber law framework (Hadjon, 2020). Through this method, the research aims to construct a comprehensive understanding of how technological advancements interact with the national criminal justice system.

Data analysis was conducted using a descriptive-analytical technique, which involves describing legal phenomena and analyzing them through relevant legal theories and principles. The statutory approach was used to interpret legislative provisions concerning cybercrime and digital evidence. In addition, a conceptual approach was adopted to clarify key concepts such as cybercrime, digital evidence, and electronic law enforcement. The study also employed a comparative approach to contrast Indonesia's cybercrime legislation with that of countries known for more advanced cyber regulations, such as the United States, South Korea, and Singapore (Rahardjo, 2021).

The analytical process aimed to identify the main barriers in Indonesia's cyber law enforcement, including limited technical expertise among law enforcement officers, weak inter-agency coordination, gaps between national legislation and technological developments, and complex issues of cross-border jurisdiction

(Hidayat, 2023). The research further examined the effectiveness of existing regulations in addressing emerging cyber threats such as phishing, ransomware, hacking, online fraud, and data breaches, all of which have become increasingly sophisticated (Ardiansyah, 2022).

In evaluating the findings, the study focused on identifying key factors influencing the effectiveness of cyber law enforcement namely institutional capacity, digital infrastructure, electronic forensic capabilities, and regulatory coherence. The results were then synthesized to formulate policy recommendations that could strengthen Indonesia's legal response to cybercrime. These include the need for enhanced training for law enforcement officers, modernization of regulatory systems, and the promotion of international cooperation to combat transnational cyber offenses (Wibowo, 2024).

By adopting this methodological framework, the study does not merely describe the existing legal structure but also critically assesses the extent to which positive law can adapt to digital transformation. The approach remains normative because it is grounded in established legal principles and statutes, yet it is also descriptive and analytical, as it reflects the empirical reality of law enforcement in Indonesia. Ultimately, this method provides a structured means of evaluating the coherence between legal norms and enforcement practices, while highlighting the areas where legal reform is essential to align with the evolving dynamics of information technology.

RESULT AND DISCUSSION

Types and Forms of Cybercrime in Indonesia

The rapid evolution of digital technology has generated a wide range of cybercrimes that are increasingly complex and difficult to control. In Indonesia, cyber offenses are no longer limited to unauthorized access or hacking but also include various illicit acts that use information technology as either the instrument or the target of crime. Common forms of cybercrime include unauthorized system intrusion, theft of personal or corporate data, dissemination of hate speech and pornographic content, online fraud, and attacks on national digital infrastructure. This trend demonstrates that cybercrime has expanded into a cross-sectoral threat, capable of disrupting economic stability, political security, and national resilience (Suryani, 2023).

Furthermore, cybercriminals employ increasingly diverse methods, ranging from phishing scams aimed at stealing user credentials, ransomware that encrypts data for ransom payments, to social engineering techniques that manipulate victims into granting system access. These offenses often overlap phishing, for instance, may lead to data theft and payment system manipulation. Such complexity complicates law enforcement, as a single act may result in multiple legal consequences (Santoso, 2022).

The enactment of Indonesia's new Criminal Code (Law No. 1 of 2023) represents a significant milestone in aligning legal frameworks with digital transformation. The code includes at least eleven provisions concerning technology-based offenses, ten of which directly regulate information technology. This codification marks a progressive step in adapting national criminal law to the digital era. However, implementation remains challenging, as many offenders exploit regulatory loopholes related to emerging technologies such as cryptocurrency, deepfakes, and artificial intelligence areas not yet explicitly governed by law (Hidayat, 2023).

Challenges in Criminal Law Enforcement in the Digital Era

Law enforcement against cybercrime in Indonesia encounters structural, technical, and substantive challenges. The first challenge lies in the regulatory gap. Although the nation has established the Electronic Information and Transactions Law (Law No. 11 of 2008) and the Personal Data Protection Law (Law No. 27 of 2022), their provisions have yet to fully address the growing complexity of cybercrime. Overlapping regulations and ambiguous legal norms often lead to uncertainty in judicial processes (Firmansyah, 2021).

Another major challenge concerns the limited technical capacity of law enforcement officers. Investigators, prosecutors, and judges frequently struggle to understand the technical intricacies of digital evidence. Electronic evidence is volatile it can be easily altered, deleted, or stored on overseas servers. The process of collecting, preserving, and analyzing such evidence requires specialized expertise in digital forensics and cyber investigation. Without these competencies, prosecutions risk being weak or even resulting in unjust verdicts (Gunawan, 2024).

Cross-border jurisdictional issues further complicate cybercrime enforcement. Many perpetrators operate abroad or use foreign-based servers, making legal action dependent on mutual legal assistance (MLA) mechanisms. However, lengthy diplomatic processes, differing legal systems, and limited bilateral agreements often delay justice (Rahardjo, 2021).

Institutional coordination also remains suboptimal. Agencies such as the National Police, Attorney General's Office, National Cyber and Encryption Agency (BSSN), Ministry of Communication and Information Technology, and Financial Services Authority (OJK) often work independently, causing overlapping authorities and fragmented responses. To ensure effective enforcement, Indonesia needs a unified command structure that integrates data, intelligence, and strategy across institutions (Rizal, 2023).

Strengthening the Legal System and Enforcement Strategies

To address these challenges, a comprehensive reform of the criminal justice system is essential, focusing on regulatory harmonization, capacity building, and international cooperation. Legal reform must ensure consistency among cyber-related laws and adapt to emerging technologies such as blockchain, artificial intelligence, and deepfakes. Updating the Electronic Information and Transactions Law in alignment with the new Criminal Code is critical to prevent contradictions and redundancies (Suryani, 2023).

Enhancing the technical capacity of law enforcement personnel is another strategic step. The government should expand specialized training in digital forensics, cybersecurity, and data analytics for investigators, prosecutors, and judges. Establishing dedicated cybercrime units equipped with advanced forensic laboratories is essential to strengthen evidence tracing and digital analysis capabilities. With adequate technological infrastructure and skilled personnel, law enforcement can become more precise and efficient (Wibowo, 2024).

Improving the reliability of digital evidence handling is equally crucial. Standardized procedures for collecting and maintaining electronic evidence must be enforced to ensure legal validity in court. The chain of custody principle should be strictly observed to track any alteration in the evidence. Moreover, explicit recognition of digital evidence forms such as metadata and server logs needs to be clarified within Indonesia's evidentiary framework (Hadjon, 2020).

On a global scale, Indonesia must enhance its participation in international cooperation to combat transnational cybercrime. Active engagement in conventions such as the Budapest Convention on Cybercrime will facilitate data exchange and extradition processes. Collaboration with international law enforcement organizations like INTERPOL and ASEANAPOL can also improve investigative coordination and effectiveness (Rahardjo, 2021).

Enhancing Digital Literacy and Social Preparedness

Beyond legal and institutional reforms, public awareness plays a vital role in mitigating cybercrime. The relatively low level of digital literacy among Indonesians is one of the primary reasons behind the increasing number of online scams and data breaches. Many victims fall prey due to poor cybersecurity habits, such as weak passwords or carelessly clicking suspicious links (Ardiansyah, 2022).

To counter this, digital literacy campaigns are essential for building a resilient cyber society. The government, in collaboration with educational institutions, private sectors, and media organizations, should launch nationwide initiatives promoting cybersecurity and digital ethics. Schools and universities must integrate cyber awareness programs into their curricula to instill responsible digital behavior from an early age. Additionally, both public and private institutions should adopt strict information security management systems to safeguard user data.

These educational measures should be reinforced with incentive-based policies for organizations that implement strong data protection standards—such as cybersecurity certifications for compliant companies. As public understanding and adherence to cybersecurity practices improve, the overall risk of cybercrime will decrease significantly (Gunawan, 2024).

Finally, continuous monitoring and evaluation of cyber law enforcement policies are needed. This includes regular audits of regulations, performance assessments of case handling, and reviews of legal infrastructure readiness in response to technological innovations. Only through adaptive and evidence-based policymaking can Indonesia's criminal justice system remain effective and relevant in the accelerating digital age.

CONCLUSION

Cybercrime poses a significant challenge to Indonesia's criminal justice system amid the rapid digitalization that permeates all aspects of modern society. While digital transformation has brought notable benefits in terms of efficiency and accessibility of information, it has also created new avenues for criminal activity exploiting technological vulnerabilities. Effective law enforcement against cybercrime therefore requires not only comprehensive legal instruments such as the Electronic Information and Transactions Law (ITE Law), the new Criminal Code (Law No. 1 of 2023), and the Personal Data Protection Law but also the readiness of law enforcement officials to understand the dynamics of the digital world and the use of electronic forensic methods in evidence gathering.

In practice, law enforcement efforts face numerous obstacles, including weak institutional coordination, limited human resource capacity in cybersecurity, and the evidentiary complexity caused by the cross-border nature and anonymity of cyber offenders. Existing regulations are often not sufficiently harmonized or adaptive to the fast-paced evolution of information technology. These conditions indicate that the challenges of cyber law enforcement in Indonesia are not only technical in nature but also systemic and structural.

To address these challenges, legal reform must focus on the digitalization of the criminal justice process, enhancement of technical and digital competencies among law enforcement officers, and the

strengthening of international cooperation in cross-border investigations. In addition, public awareness of cybersecurity must be improved through education initiatives and national digital literacy programs. The synergy between regulation, technology, and legal awareness within society is essential to maintaining a balance between legal protection and digital freedom in the modern era.

Ultimately, the effectiveness of cyber law enforcement in Indonesia depends on the ability of the national legal system to adapt responsively and progressively to technological developments. The digital era not only demands updates to legal norms but also requires a paradigm shift in law enforcement toward a system that is more inclusive, intelligent, and grounded in electronic evidence.

REFERENCES

Aldriano, M., & Priyambodo, R. (2022). Teknologi informasi dan implikasinya terhadap sistem hukum nasional. Jurnal Hukum & Teknologi, 5(3), 112–128. https://doi.org/10.35791/jht.2022.5.3.112

Azzahra, N. (2025). Cybercrime di Indonesia: Analisis hukum dan tantangan penegakan hukum digital. Jurnal Keamanan Siber Indonesia, 4(1), 21–39. https://doi.org/10.47266/jksi.2025.v4i1.21

Badan Siber dan Sandi Negara. (2024). Laporan tahunan serangan siber nasional 2024. Jakarta: BSSN Press.

Budapest Convention on Cybercrime. (2001). Council of Europe Treaty Series No. 185. Strasbourg: Council of Europe.

Dinda, A. (2024). Dinamika penegakan hukum terhadap kejahatan siber di Indonesia. Jurnal Penelitian Hukum Digital, 3(2), 45–63. https://doi.org/10.31092/jphd.2024.v3i2.45

Hidayat, M. (2023). Digitalisasi hukum pidana dalam menghadapi era revolusi industri 4.0. Jurnal Ilmu Hukum dan Teknologi, 8(1), 55–73. https://doi.org/10.31219/jht.2023.8.1.55

Hukumonline. (2023). Pokok-pokok perubahan dalam KUHP baru dan implikasinya terhadap kejahatan digital. Diakses dari https://www.hukumonline.com/berita/kuhp-baru-digitalisasi

Judijanto, T., & Nugroho, S. (2025). Penegakan hukum lintas batas terhadap cybercrime di Indonesia. Jurnal Hukum Siber dan Keamanan Digital, 6(2), 88–107. https://doi.org/10.46747/jhskd.2025.v6i2.88

Kementerian Komunikasi dan Informatika. (2024). Strategi nasional keamanan siber Indonesia 2024–2029. Jakarta: Direktorat Keamanan Informasi Kominfo.

Mahfud, M. D. (2022). Politik hukum di Indonesia dalam menghadapi era digital. Jakarta: Rajawali Pers.

Marzuki, P. M. (2020). Penelitian hukum: Pendekatan normatif dan empiris (Edisi Revisi). Jakarta: Prenada Media.

Rayyan, A. (2024). Transformasi hukum pidana dalam menghadapi era digitalisasi: Perspektif kritis terhadap KUHP baru. Jurnal Reformasi Hukum, 7(1), 99–118. https://doi.org/10.47123/jrh.2024.v7i1.99

Soedirman Law Review. (2023). Analisis efektivitas penegakan hukum terhadap pelanggaran UU ITE di Indonesia. Soedirman Law Review, 5(2), 120–137. https://doi.org/10.25077/slr.2023.5.2.120

Sudarto. (2021). Hukum pidana dan pembaruan sistem peradilan di Indonesia. Bandung: Citra Aditya Bakti.

Sutedi, A. (2022). Aspek hukum kejahatan siber dan penegakannya di Indonesia. Depok: Rajagrafindo Persada.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 32).

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58).

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251).

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 182).

Universitas Gadjah Mada. (2023). Laporan penelitian: Tingkat penegakan hukum terhadap kejahatan siber di Indonesia. Yogyakarta: UGM Center for Cybercrime Studies.

We Are Social. (2024). Digital 2024: Indonesia report. DataReportal. https://datareportal.com/reports/digital-2024-indonesia