Journal of Law and Regulation Governance

Proving Illegal Access in Combating Cybercrime in Indonesia

Rifi Noor Faizal Tombolotutu[1], Tofik Yanuar Chandra[2], Hedwig Adianto Mau[3]
Universitas Jayabaya, Jakarta Timur, Indonesia[1,2,3]
Email: lavistaaa93@gmail.com, tyc.jayabaya@gmail.com,
hedwigadiantomau@pascajayabaya.ac.id

ABSTRACT

The development of information and communication technology has led to the existence of new media in the form of the internet which causes world relations to become borderless and causes significant social, economic, and cultural changes and even crimes in the field of the internet are increasing. The formulation of the problem that will be raised as a problem in this study is How to prove illegal access in the prevention of cybercrime in Indonesia? And what is the process of investigating illegal access cases in the prevention of cybercrime in Indonesia? The research method used is normative juridical with a case, legislation and concept research approach. The legal materials used are primary, secondary and tertiary, while the analysis of qualitative legal materials is qualitative. The results of the study show that proving illegal access in handling cybercrime cases in Indonesia still faces various challenges, especially in terms of identifying perpetrators and limited human resources. However, with the right strategies, including increased international cooperation, the use of advanced technology, and ongoing training, these challenges can be overcome. Revision of existing policies and increasing the capacity of law enforcement are the main keys in increasing the effectiveness of cybercrime countermeasures. The process of investigating illegal access cases in Indonesia requires an integrated approach, involving sophisticated forensic technology, understanding of legal regulations, and international cooperation. By integrating criminological theories such as Routine Activity and Strain, as well as leveraging insights from the current literature and best practices, law enforcement can improve their ability to deal with cybercrime.

Keywords: illegal access, cybercrime, cybercrime countermeasures

INTRODUCTION

The rapid development of technology and the need for everyone to be more open to technology from time to time, can make a person with malicious intentions to abuse information technology for various reasons and specific purposes (Nugraha, Lukitaningtyas, Ridho, Wulansari, & Al Romadhona, 2022). The sophisticated and fast use of the internet also gives rise to crimes that are very sophisticated and difficult to find out the perpetrators, this is because the internet is an invisible communication medium (virtual), so that criminals can easily eliminate traces without being able to clearly know the purpose and motive of the crime committed.

Unlawful acts in cyberspace are a very worrying phenomenon, considering that acts of *carding*, *hacking*, fraud, terrorism and the spread of destructive information have become part of

criminal activities in cyberspace. In fact, this is in stark contrast to the absence of regulations that regulate the use of information and communication technology in various sectors, therefore to ensure legal certainty, the government is obliged to regulate various activities related to the use of information and communication technology through the use of the internet (Ulya & Musyarri, 2020).

The crime of using the internet with illegal access is a form of *cyber crime* where *cyber crime* has shown its real appearance in the world of advanced technology products such as the internet or computers (McCusker, 2017). This reality shows that the offer of progress in the era of globalization, in addition to bringing benefits or positive values, also contains dangerous contents for the life of the community and the nation.

There has been an increase in *illegal* access crimes as a form of cybercrime in the ranks of the Cyber Directorate of the National Police Criminal Investigation Department, in 2020 there were 201 cyber cases, in 2021 there was an increase to 612 cyber cases and in 2022 there was a significant increase to 8,831 cyber cases compared to the previous year. The highest number of cyber cases in 2022 were fraud crimes with 134 cases, defamation with 125 cases, and hate speech with 120 cases. The following is the cybercrime in Indonesia that has increased many times (Polri, 2022).

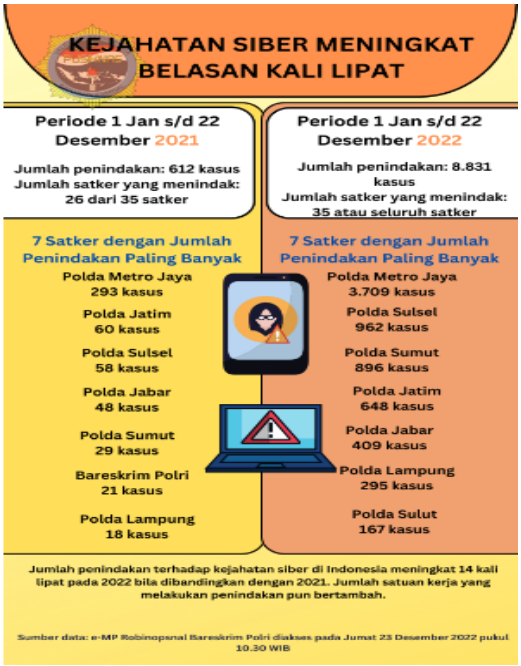

Figure 1.
Source : https://pusiknas.polri.go.id (2022)

The various modus operandi of *cybercrime* with illegal access carried out by bank robbers must be immediately anticipated by the legal apparatus in Indonesia, fast work and careful proof must be able to be done so that the law does not look weak. Bank break-in is a type of white *color*

crime committed by intellectuals by utilizing the sophistication of computer technology and strategies as well as loopholes in the bank's internal rules and applicable legal rules (Schneier, 2023).

One of the crimes is *Illegal Access*, which is highly dependent on the lifestyle or technological advances that develop in a society that is more popular with the term cyber crime (Saridakis, Benson, Ezingeard, & Tennakoon, 2016). The phenomenon that has occurred recently occurred on January 16 and January 19, 2022 in the city of Solo with a case of alleged credit card break-in committed by a person who has expertise in the field of hackers. Because in just a moment the perpetrator was able to break into 4 credit cards belonging to only one person, namely on January 16 at night, three credit cards with different pin numbers could be broken into up to 24 transactions with a loss of Rp 120.2 million, while the other credit card break-in occurred again on January 19 in one transaction with a loss of Rp 13.9 million. For the break-in incident, the total loss amounted to Rp 134 million until the contents of the credit card were all drained. The existence of this incident indicates that credit card crime is a threat to the wider community, especially those who have credit cards (Ibrahim, 2022).

Until now, with the increasingly widespread use of computer network technology, crimes in the computer field are also increasing, many cases occur, but not many have reached the courts (Smith, 2018). One of the problems faced by law enforcement to ensnare perpetrators is the problem of proving the guilt of the defendant. This reality is a challenge for legal circles that must be accepted to solve all problems that occur due to the rapid development of technology. Crime using information technology, especially the internet, has reached an alarming stage. The advancement of information technology, in addition to bringing to the revolutionary business world the Digital Revolutioner Area, which is all practical, also has a terrible dark side such as computer crime, pornography, terrorism, gambling, fraud, theft, the spread of hoax news, and so on. Proof is a matter that plays a role in the examination process of the court hearing, with this proof determining the fate of the defendant (Bielen, Grajzl, & Marneffe, 2017). If the results of the proof with the evidence prescribed by law are not enough to prove the guilt charged to the defendant, the defendant is exempt from punishment, on the other hand, if the defendant can be proven by the evidence mentioned in Article 184 of the Criminal Code, the defendant must be found guilty and he will be sentenced. Therefore, judges must be careful, meticulous, and mature in assessing and considering the issue of proof. Examining the minimum limit of "evidentiary power" or "bewijs kracht" of each piece of evidence mentioned in Article 184 of the Criminal Procedure Code.

As stated above, the evidentiary process aims to prove whether the defendant is guilty or not. In that context, what must be proven is the criminal act or criminal act and criminal liability (Stoykova, 2023). In practice, due to the complexity of the case, sometimes it is not easy to determine a crime of premeditated murder. Therefore, the definition and requirements of the planning element in the debate between pro and con parties are always dynamic. The debate in

question is the proof of motive elements in the crime of premeditated murder. The proponents say the motive must be proven while the counters say the motive does not need to be proven.

RESEARCH METHODS

Normative law research essentially examines the law that is conceptualized as a norm or rule that applies in society, and becomes a reference for everyone's behavior. According to Soerjono Soekanto and Sri Mamudji, normative legal research is legal research that is carried out by researching literature materials or secondary data. Based on the explanation above, the researcher decided to use the normative legal research method to research and write this thesis discussion as a legal research method The use of normative research methods in research efforts and thesis research is motivated by theoretical compatibility with the research methods needed by the researcher.

The research approach used in this study is a qualitative approach because the problem to be studied examines a process about proving illegal access in the prevention of cybercrime in Indonesia. The research approach used is as follows: legislative approach, concept and case approach. The sources of legal materials used are primary, secondary and tertiary. Analysis of legal materials is qualitative.

RESULTS AND DISCUSSION

Proving Illegal Access in Cybercrime Mitigation in Indonesia

Proving illegal access in countering cybercrime in Indonesia is one of the important aspects in ensuring justice and security in the digital era (Nadriana & Sukmana, 2022). This phenomenon refers to the act of accessing computer systems or networks without permission, which is regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), which was later updated with Law Number 19 of 2016. Article 30 of the ITE Law states that any person who intentionally and without rights or against the law accesses another person's computer and/or electronic system can be subject to criminal sanctions. Proving a case of illegal access requires several key elements: the act of access itself, the absence of permission from the owner or manager of the system, and the intentionality of the act. Evidence that can be used includes electronic documents such as emails and system logs, statements from information technology experts, witnesses who knew or experienced the event, and additional clues such as suspicious access patterns (Kohlhepp, 2021). The results of the researcher's interview with the Head of the Directorate of Cyber Crime of the Criminal Investigation Branch of the National Police Headquarters are related to the main challenges faced in proving illegal access in cybercrime cases in Indonesia, namely:

> *"..The main challenge we face is identifying and tracking down perpetrators who often use sophisticated techniques to hide their tracks. For example, the perpetrator could use a VPN, proxy, or encryption method that is difficult to track. In addition, the limitations of human resources and technology at the Directorate of Cyber Crime are also a major obstacle. We*

need more trained digital forensics experts and more advanced tools to analyze digital evidence.." (Pimpinan Direktorat Tindak Pidana Siber Bareskrim Mabes Polri)

Analysis of the results of proving illegal access shows that cyber law enforcement in Indonesia still faces various significant challenges (Rafie, Merta, & Junaidi, 2024). To address these challenges, various strategies have been implemented by law enforcement. One of the main strategies is to increase international cooperation with law enforcement agencies in other countries as well as global technology companies. This cooperation allows for the exchange of information, technical support, and training that Indonesia cannot access independently. For example, cooperation with Interpol or international cybersecurity companies has proven effective in some cases.

In addition, the use of sophisticated digital forensic tools is key in collecting, analyzing, and storing digital evidence. Advanced system log analysis software, for example, can help identify patterns of illegal access and link criminal activity to perpetrators. Law enforcers also routinely conduct ongoing training to improve their technical skills in the field of digital forensics and cybersecurity (Humphries, Nordvik, Manifavas, Cobley, & Sorell, 2021). This training includes an understanding of the latest methods used by cybercriminals, as well as the use of cutting-edge digital forensic tools.

Rapidly evolving technologies often exceed law enforcement's ability to keep pace with new threats, requiring increased capacity and resources. In addition, cybercrime that is transnational requires strong international cooperation. Research in journals such as the Journal of Cybersecurity and Computer Law & Security Review shows that collaboration between law enforcement, academia, and the private sector is essential to creating effective countermeasure strategies. Relevant theories, such as the Routine Activity theory and the Strain theory, also help understand the motivations and behavioral patterns of cybercriminals, so that law enforcement can design a more targeted approach (Sarkar & Shukla, 2023). Then how is the strategy used by the Directorate of Cybercrime in overcoming this challenge, the researcher conducted an in-depth interview with Cyber Crime Investigators consisting of the Head of Sub-Directorate I, as follows :

"...One of our key strategies is to increase international cooperation with law enforcement agencies in other countries as well as global technology companies. This cooperation helps us get technical support and information that we can't access on our own. In addition, we also hold regular training to improve the technical skills of our members in the use of digital forensic tools. The use of sophisticated system log analysis software is also an important part of our strategy in gathering evidence.."

Case studies from various countries show that success in tackling cybercrime often depends on the use of advanced technology to detect and analyze digital footprints, as well as ongoing training for law enforcement. For example, in a study published in *the "International Journal of Cyber Criminology"*, it was explained how the use of digital forensic tools can speed up the process of identifying and proving cases of illegal access. In addition, the role of the State Cyber and Cryptography Agency (BSSN) in Indonesia in maintaining national cyber security is very vital. This

institution collaborates with the Directorate of Cyber Crime in the Police and the Ministry of Communication and Information Technology (Kominfo) to ensure effective regulations and policies. The results of an interview with one of the law enforcers of the Head of Sub-Directorate III of the Directorate of Cyber Crime in the Police related to the effectiveness of the ITE Law in supporting the proof of illegal access, are as follows :

> *"…The ITE Law has provided an important legal basis for us to handle cybercrime cases. However, there are some gaps that need to be fixed. For example, the definition and technical rules regarding the collection and storage of digital evidence still need to be clarified. In addition, coordination between law enforcement agencies is often a problem due to complicated bureaucracy. Therefore, we hope that there will be revisions and improvements in the ITE Law to better support technical needs in proving cases of illegal access.."(Kasubdit III)*

From the results of interviews with law enforcement officers of the Head of Sub-Directorate III of the Directorate of Cyber Crime in the Police, it was revealed that one of the main challenges in proving illegal access is the difficulty in identifying and tracking the perpetrators. Through the ITE Law, it provides an important legal basis for proving illegal access in Indonesia. Article 30 of the ITE Law provides a clear definition of illegal access and establishes criminal sanctions for violators, providing a comprehensive framework for law enforcement. However, there are several weaknesses in its implementation. Lack of clarity in technical definitions and procedures for collecting and analyzing digital evidence can create difficulties for law enforcement (Arshad, Jantan, & Abiodun, 2018). In addition, coordination between law enforcement agencies is often hampered by complicated bureaucracy, hindering the effectiveness of handling cybercrime cases.

To address these weaknesses, several policy recommendations can be proposed. First, there is a need for a revision of the ITE Law to clarify the technical definition and add more detailed articles related to the collection and analysis of digital evidence. Second, governments should invest in ongoing training and increased resources for law enforcement, as well as develop technological infrastructure that supports cyber law enforcement. Third, policies that facilitate better coordination between law enforcement agencies and related agencies must be implemented to simplify bureaucracy and increase collaboration.

Proving illegal access faces significant challenges. One of the main challenges is the identification and tracking of actors who often use sophisticated techniques such as VPNs (Virtual Private Networks), proxies, and encryption to hide their tracks. These techniques make the digital footprint left by the perpetrator difficult to trace, making the evidentiary process difficult. In addition, the Directorate of Cyber Crime in the Police often faces a limited number of human resources trained in the field of digital forensics as well as the limitations of advanced technological tools needed to analyze digital evidence.

The Electronic Information and Transaction Law (UU ITE) is the main legal basis in combating cybercrime in Indonesia, including illegal access. Proof of illegal access, which refers to the act of entering or using a computer system without permission, relies heavily on the provisions

stipulated in the ITE Law. The ITE Law, specifically Article 30, provides a clear definition of illegal access and establishes criminal sanctions for violators. This provides a strong legal basis for law enforcement to process related cases. The ITE Law recognizes the validity of electronic evidence, such as system logs and digital documents. This is especially important in the context of proving illegal access, where the primary evidence is often digital.

Evolving technology allows perpetrators to hide their digital footprint more effectively. In addition, the lack of trained human resources in the field of digital forensics also hampers the investigation process. Law enforcement also revealed that existing regulations have not fully supported the technical needs in proving cases of illegal access (Arshad et al., 2018). Real cases that have been handled by the Directorate of Cyber Crime in the Police show that the effectiveness of the ITE Law is highly dependent on technical capabilities and international cooperation. In some cases, such as attacks on major banks or e-commerce companies, cooperation with international cybersecurity companies and the use of advanced digital forensic tools have helped gather strong evidence. However, regulatory and resource limitations are still an obstacle in many other cases.

Overall, proving illegal access in the fight against cybercrime in Indonesia requires a holistic approach that combines aspects of law, technology, and international collaboration. By continuing to improve law enforcement capabilities through adequate training and resources, as well as strengthening cooperation between countries, Indonesia can more effectively deal with the increasingly complex threat of cybercrime. Support from the scientific literature and academic research is also a strong basis for developing more effective and sustainable countermeasures.

This analysis is supported by several theories of criminology and digital forensics. The Routine Activity Theory explains that crimes occur when there are motivated perpetrators, available targets, and a lack of adequate supervision (Stadnicki, Corsini, & Szulkin, 2024). In the context of illegal access, perpetrators take advantage of weaknesses in the security system to commit crimes. Strain Theory (2015) links social and economic pressures to criminal behavior, explaining that some cybercriminals are driven by economic factors that drive them to seek profit through illegal activities. Strain Theory, developed by Robert K. Merton, states that individuals who experience an inability to achieve goals valued by society through legitimate means may turn to criminal behavior (Unnever, Gabbidon, & Chouhy, 2019).

This research and analysis is also supported by various relevant journals and literature. "*Cybercrime and Society*" by David S. Wall provides a comprehensive view of the dynamics of cybercrime and challenges in law enforcement, including the proof of illegal access (Wall, 2015). "Digital Evidence and Computer Crime" by Eoghan Casey discusses in depth digital forensics and the importance of digital evidence in cyber law enforcement. The journal "*Challenges and Solutions in Cyber-Forensics*" (*Journal of Digital Forensics, Security and Law*) reviews the challenges in digital forensics and the strategies used to address these problems (Roussev, 2016). The article "International Collaboration in Cybercrime Investigation" (International Journal of Cyber Criminology) highlights the importance of international cooperation in cybercrime investigation and

its relevance in proving illegal access in Indonesia (Cascavilla, Tamburri, & Van Den Heuvel, 2021).

According to researchers, proving illegal access in countering cybercrime in Indonesia is a key aspect in ensuring the effectiveness of law enforcement in the digital era. Illegal access, i.e. the act of entering a computer system without permission, presents complex challenges for law enforcement, especially in the context of increasingly sophisticated cybercrime. The handling of these cases requires an in-depth and multidimensional approach, involving advanced forensic technology, a detailed understanding of the law, and solid international coordination.

Overall, proving illegal access in cybercrime prevention in Indonesia requires integration between criminological theory, forensic technology, and international cooperation. By using a comprehensive, theory-based approach, and leveraging insights from the current literature, law enforcement can improve their effectiveness in handling and proving cases of illegal access.

Investigation Process of Illegal Access Cases in Cybercrime Remediation in Indonesia

In today's digital era, cybercrime, especially illegal access, is a significant challenge for law enforcement in Indonesia. Illegal access refers to the act of entering a computer system or network without permission, which can cause significant losses both financially and reputationally. The process of investigating illegal access cases requires a comprehensive approach, involving forensic technology, legal regulations, and international cooperation. This sub-chapter will discuss the process of investigating illegal access cases by analyzing the investigation steps, the challenges faced, and the role of criminological theory in understanding and handling these cases.

The process of investigating illegal access cases in cybercrime prevention in Indonesia is a complex and multidimensional effort, involving various technical, legal, and administrative elements. Illegal access, which includes the unauthorized act of accessing a computer system or network, requires an integrated approach to ensure that perpetrators can be identified and acted upon effectively. The process begins with the identification of violations, followed by the collection and analysis of digital evidence, and involves legal considerations and international cooperation.

1. **Digital Evidence Collection and Processing**

   The collection of digital evidence is a crucial first step in the investigation of illegal access cases. This process must be carried out carefully to ensure that all relevant data is collected and its integrity is protected. Referring to "Challenges and Solutions in Cyber-Forensics" by Bertino and Sandhu (2015), digital forensic techniques such as disk imaging and log analysis are the main tools used to collect evidence (Khokhar, Iqbal, Fung, & Bentahar, 2020). The use of sophisticated forensic software allows investigators to extract data from compromised systems without damaging the evidence. Moreover, techniques such as deleted data recovery and metadata analysis help in the reconstruction of the digital footprint of the perpetrator. The process of collecting and processing evidence must adhere to strict forensic procedures to ensure that the resulting evidence is admissible in court.

2. **Forensic Analysis and Digital Trace Reconstruction.**

Once the evidence has been collected, the next stage is forensic analysis, which involves reconstructing the perpetrator's activities based on digital evidence. The book *"Cybercrime and Society"* by David S. Wall (2017) emphasizes the importance of forensic analysis in understanding access patterns carried out by perpetrators (Wall, 2017). These analysis techniques include tracing activity logs, reconstructing deleted data, and identifying suspicious patterns. Investigators must be able to relate visible digital activities to specific actions taken by the perpetrator to build a solid case. This analysis also involves verifying the authenticity of the data and ensuring that all the evidence produced is free of contamination.

3. **Legal and Regulatory Challenges.**

Investigations into illegal access also face significant legal challenges. The ITE Law in Indonesia provides a legal framework for handling cybercrime, but its implementation often faces obstacles related to technical definitions and forensic procedures. In this context, the *Routine Activity* theory by Cohen and Felson (2015) provides insight into how cybercrime occurs when there are deficiencies in system oversight. To overcome this challenge, there is a need for rapid regulatory updates to keep up with the development of new technologies and methods of crime. Investigators should also work closely with policymakers to ensure that existing laws are adequate to handle cybercrime cases.

4. **International Coordination and Cooperation.**

International cooperation is a key element in the investigation of illegal access cases, especially since cybercrime often involves perpetrators from various countries. The article "*International Collaboration in Cybercrime Investigation"* by Zhang and Liu (2015) in the *International Journal of Cyber Criminology* emphasizes the importance of coordination between international and national law enforcement agencies. This cooperation includes the exchange of information, investigative techniques, and resources to improve the effectiveness of investigations. Strengthening international networks and harmonizing forensic and legal standards between countries helps in handling cases involving cross-border actors and global infrastructure. In order for the investigation process to run effectively, it is important to keep the investigators' skills and knowledge updated regarding the latest technology and forensic techniques. Ongoing training and capacity building in digital forensics are integral to law enforcement efforts. Education and training obtained from literature such as "Cybercrime and Society" ensure that law enforcement personnel can face new challenges with adequate expertise. The use of the latest forensic techniques and appropriate analysis tools will improve the ability of investigators to address cases of illegal access.

According to the researcher's analysis, the process of investigating illegal access cases in Indonesia requires a comprehensive and theory-based approach. By leveraging insights from criminological theory, forensic technology, and international cooperation, law enforcement can improve the effectiveness of cybercrime investigations and countermeasures. Strengthening forensic procedures, updating regulations, and expanding international cooperation are important steps in improving law enforcement's ability to deal with the ever-evolving cybercrime.

CONCLUSION

Based on the description above, it can be concluded that, first, proving illegal access in handling cybercrime cases in Indonesia still faces various challenges, especially in terms of identification of perpetrators and limited human resources. However, with the right strategies, including increased international cooperation, the use of advanced technology, and ongoing training, these challenges can be overcome. Revision of existing policies and increasing the capacity of law enforcement are the main keys in increasing the effectiveness of cybercrime countermeasures. Second, the process of investigating illegal access cases in Indonesia requires an integrated approach, involving sophisticated forensic technology, understanding of legal regulations, and international cooperation. By integrating criminological theories such as Routine Activity and Strain, as well as leveraging insights from the current literature and best practices, law enforcement can improve their ability to deal with cybercrime. Strengthening forensic procedures, updating regulations, and expanding international cooperation are important steps in improving the effectiveness of cyber crime investigations and countermeasures in Indonesia.

REFERENCES

Arshad, H., Jantan, A. Bin, & Abiodun, O. I. (2018). Digital forensics: review of issues in scientific validation of digital evidence. *Journal of Information Processing Systems*, 14(2), 346–376.

Bielen, S., Grajzl, P., & Marneffe, W. (2017). Procedural events, judge characteristics, and the timing of settlement. *International Review of Law and Economics*, 52, 97–110. Retrieved from https://doi.org/10.1016/j.irle.2017.09.001

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W.-J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, 105, 102258. Retrieved from https://doi.org/10.1016/j.cose.2021.102258

Humphries, G., Nordvik, R., Manifavas, H., Cobley, P., & Sorell, M. (2021). Law enforcement educational challenges for mobile forensics. *Forensic Science International: Digital Investigation*, 38, 301129. Retrieved from https://doi.org/10.1016/j.fsidi.2021.301129

Ibrahim, M. W. (2022). Cara Dan Syarat bisnis hingga potensi keuntungan franchise indomaret, Solopos. com. Solopos. com. Available at: https://www. solopos. com/cara-dan-syarat-bisnis ….

Khokhar, R. H., Iqbal, F., Fung, B. C. M., & Bentahar, J. (2020). Enabling secure trustworthiness assessment and privacy protection in integrating data for trading person-specific information. *IEEE Transactions on Engineering Management*, 68(1), 149–169.

Kohlhepp, B. (2021). Investigations: Use of DNA and Fingerprints. In *Encyclopedia of Security and Emergency Management* (pp. 614–621). Springer.

McCusker, R. (2017). Transnational organised cyber crime: distinguishing threat from reality. In *Transnational Financial Crime* (pp. 415–432). Routledge.

Nadriana, L., & Sukmana, P. (2022). Exploring the Applicability of Common Law Principles in Combating Cybercrime in Indonesia: An Analysis of Current Legal Framework and Challenges. *International Journal of Cyber Criminology*, 16(2), 192–204.

Nugraha, A. A., Lukitaningtyas, Y. K. R. D., Ridho, A., Wulansari, H., & Al Romadhona, R. A. (2022). Cybercrime, Pancasila, and Society: Various Challenges in the Era of the Industrial Revolution 4.0. *Indonesian Journal of Pancasila and Global Constitutionalism*, 1(2), 307–390.

Polri, P. B. (2022). Kejahatan Siber di Indonesia Naik Berkali-kali Lipat. *Pusiknas. Polri. Go. Id. Https://Pusiknas. Polri. Go. Id/Detail_artikel/Kejahatan_siber_di_indonesia_naik_berkali-Kali_lipat*.

Rafie, P. A., Merta, M. M., & Junaidi, J. (2024). The Enforcement Of Cybercrime Law Within The Legal System Of Indonesia. *Journal Of Humanities, Social Sciences And Business*, 3(3), 594–600.

Roussev, V. (2016). *Digital forensic science: issues, methods, and challenges*. Morgan & Claypool Publishers.

Saridakis, G., Benson, V., Ezingeard, J.-N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, 102, 320–330. Retrieved from https://doi.org/10.1016/j.techfore.2015.08.012

Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, 2, 100034. Retrieved from https://doi.org/10.1016/j.jeconc.2023.100034

Schneier, B. (2023). *A hacker's mind: how the powerful bend society's rules, and how to bend them back*. WW Norton & Company.

Smith, R. (2018). *Crime in the digital age: Controlling telecommunications and cyberspace illegalities*. Routledge.

Stadnicki, I., Corsini, M., & Szulkin, M. (2024). Application of criminology in urban ecology and evolution: Routine Activity Theory and field equipment disappearance dynamics. *Ecological Indicators*, 165, 112095. Retrieved from https://doi.org/10.1016/j.ecolind.2024.112095

Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law & Security Review*, 49, 105801. Retrieved from https://doi.org/10.1016/j.clsr.2023.105801

Ulya, N. U., & Musyarri, F. A. (2020). Reformulasi Pengaturan Mengenai Financial Technology Dalam Hukum Positif Di Indonesia. *Arena Hukum*, 13(3), 479–500.

Unnever, J., Gabbidon, S., & Chouhy, C. (2019). *Building a Black Criminology*. Routledge.

Wall, D. S. (2015). Dis-organised crime: Towards a distributed model of the organization of cybercrime. *The European Review of Organised Crime*, 2(2).

Wall, D. S. (2017). *Cyberspace crime*. Routledge.