THE ROLE OF SURVEILLANCE TECHNOLOGY IN THE INVESTIGATION PROCESS OF CYBER CRIMES: A LEGAL PERSPECTIVE IN INDONESIA

Dwiningsih Maryanti[1], Dwi Saputra Ardianto[2], Dian Mustika[3]
UIN Mataram[1], Universitas Bung Hatta Padang[2], Universitas Merdeka Malang[3]
dwiningsihmaryanti614@gmail.com[1], dwisaputra88@gmail.com[2], mustikadian@gmail.com[3]

Abstrak:

Perkembangan teknologi digital telah memberikan dampak signifikan terhadap berbagai aspek kehidupan, termasuk dalam bidang penegakan hukum. Di Indonesia, tindak pidana siber semakin kompleks, menuntut adanya pendekatan penyidikan yang lebih canggih dan efektif. Salah satu pendekatan yang diadopsi adalah penggunaan teknologi pengawasan dalam proses penyidikan. Artikel ini mengeksplorasi peran teknologi pengawasan dalam penyidikan tindak pidana siber, dengan fokus pada perspektif hukum di Indonesia. Melalui analisis yuridis, artikel ini mengidentifikasi jenis-jenis teknologi pengawasan yang digunakan oleh aparat penegak hukum, seperti perangkat lunak pengintai, pemantauan aktivitas daring, dan analisis data besar. Artikel ini juga mengkaji implikasi hukum dari penggunaan teknologi tersebut, termasuk masalah privasi, legalitas bukti elektronik, dan tantangan dalam memastikan kepatuhan terhadap peraturan hukum yang berlaku. Dalam konteks Indonesia, artikel ini menyoroti perlunya regulasi yang lebih spesifik dan jelas untuk mengatur penggunaan teknologi pengawasan agar tidak melanggar hak asasi manusia, serta pentingnya pelatihan bagi penyidik dalam mengoperasikan teknologi tersebut. Dengan demikian, artikel ini memberikan pandangan mendalam mengenai dinamika penggunaan teknologi pengawasan dalam penyidikan tindak pidana siber di Indonesia dan relevansinya dalam penegakan hukum yang adil dan efektif.

Kata kunci: Teknologi Pengawasan, Penyidikan, Tindak Pidana Siber

Abstract:

The development of digital technology has had a significant impact on various aspects of life, including in the field of law enforcement. In Indonesia, cybercrime is increasingly complex, demanding a more sophisticated and effective investigative approach. One of the approaches adopted is the use of surveillance technology in the investigation process. This article explores the role of surveillance technology in the investigation of cybercrimes, focusing on legal perspectives in Indonesia. Through juridical analysis, this article identifies the types of surveillance technologies used by law enforcement officials, such as surveillance software, online activity monitoring, and big data analysis. The article also examines the legal implications of using such technologies, including privacy concerns, the legality of electronic evidence, and the challenges of ensuring compliance with applicable laws and regulations. In the context of Indonesia, this article highlights the need for more specific and clear regulations to regulate the use of surveillance technology so as not to violate human rights, as well as the importance of training for investigators in operating such technology. Thus, this article provides an in-depth look at the dynamics of the use of surveillance technology in the investigation of cybercrime in Indonesia and its relevance in fair and effective law enforcement.

Keywords: Surveillance Technology, Investigation, Cyber Crime

INTRODUCTION

The development of information and communication technology has brought significant changes in various aspects of life, including in the field of law. In Indonesia, these technological advances have created new challenges in law enforcement, especially related to cybercrime. Cybercrime, which includes various forms of crime committed through or by utilizing digital technology, has become a serious concern for law enforcement. With the increasing use of the internet and digital devices, cybercrime is increasingly complex and difficult to detect, requiring a more innovative approach to the investigation process. One such approach is the use of surveillance technology as a tool in uncovering and collecting evidence of cybercrime (Lestari & Damayanti, 2018).

Surveillance technology includes a variety of tools and techniques used to monitor, record, and analyze activities carried out digitally. In the context of cyber crime investigations, this technology plays a crucial role in identifying perpetrators, tracking digital traces, and collecting evidence that can be used in court. Some forms of surveillance technology that are often used include spyware, network monitoring, and big data analytics. Although this technology provides many benefits in law enforcement efforts, its use also raises various complex legal issues, such as privacy issues, the legality of the evidence obtained, and the potential for misuse (Flora et al., 2024).

The issue of privacy is one of the main challenges in the use of surveillance technology. In the investigation process, this technology often involves collecting personal data without the knowledge or consent of the data owner. This raises questions about the extent to which states can restrict individual privacy rights in the interests of law enforcement. In Indonesia, data privacy regulations are still not fully comprehensive, opening up space for potential human rights violations. Therefore, it is important to examine whether the use of surveillance technology in the investigation of cybercrime has been in accordance with applicable legal principles and how regulations can be strengthened to protect individuals' privacy rights (Soraja, 2021).

In addition to privacy issues, the legality of evidence obtained through surveillance technology is also a concern. In the criminal justice system, evidence obtained illegally or illegally cannot be used in a trial. However, with the increasing complexity of the technology used in cybercrime, law enforcement is often faced with the dilemma of obtaining strong evidence and adhering to strict legal procedures. In Indonesia, laws related to electronic evidence are still in the development stage, and many cases show uncertainty regarding the receipt of evidence obtained through surveillance technology. Therefore, a study of the legal framework that regulates the use of electronic evidence is urgently needed to ensure fairness in the judicial process (Sianipar & Sembiring, 2024).

In addition to the legality aspect, the use of surveillance technology also poses challenges in terms of operationalization in the field. Law enforcement must have adequate skills and knowledge to operate this technology effectively. Without adequate training, surveillance technology can be misused or not used optimally, which can ultimately harm the investigation process. In Indonesia, training and capacity building for investigators in the use of surveillance technology still need to be improved. These efforts are not only important to improve the effectiveness of investigations, but also to ensure that the technology is used in accordance with ethical and legal standards (Syam et al., 2023).

In the face of these challenges, it is important for Indonesia to develop more specific and clear regulations related to the use of surveillance technology in the investigation of cybercrimes. These regulations must include aspects related to privacy protection, the legality of evidence, and operational standards that law enforcement must adhere to. In addition, there needs to be an effective monitoring mechanism to ensure that the use of surveillance technology does not violate human rights and remains within the applicable legal corridor. The development of comprehensive regulations will be an important step in ensuring that surveillance technology can be used effectively and fairly in the law enforcement process (Bambang et al., 2021).

Therefore, this article aims to explore the role of surveillance technology in the process of investigating cybercrimes in Indonesia, with a focus on legal perspectives. Through this study, it is hoped that it can provide a clear picture of the dynamics of the use of surveillance technology in investigations, as well as its implications for the legal system in Indonesia. Researchers will also discuss the various challenges faced in the application of this technology, as well as recommendations to strengthen existing regulations and practices in order to achieve fair and effective law enforcement (Malau, 2023).

METHOD

This study uses a normative juridical approach with a focus on analyzing laws and regulations related to the use of surveillance technology in the investigation process of cyber crimes in Indonesia. The normative juridical approach was chosen because of the relevance of this method in examining the written legal rules governing the use of surveillance technology and its relation to human rights and criminal justice processes. In conducting the analysis, this research uses primary legal materials, such as laws, government regulations, and other regulations related to cyber crime and surveillance technology. In addition, secondary legal materials, such as journals, books, and articles discussing related issues, are also used as references to enrich the analysis.

Data collection is carried out through document studies of relevant laws and regulations and literature. The data obtained from the study of this document is then analyzed qualitatively to identify and evaluate various legal issues that arise in the use of surveillance technology. This analysis aims to understand how existing regulations regulate the use of surveillance technology, as well as to identify legal gaps or potential problems that may arise. In the analysis process, this study also considers relevant court decisions, in order to understand how the law is applied in real cases involving surveillance technology.

To support normative analysis, this study also conducts in-depth interviews with legal experts and practitioners who have experience in the field of cyber crime investigation. This interview aims to gain practical views on the application of surveillance technology in the field as well as the challenges faced by law enforcement. The results of this interview are then combined with juridical analysis to provide a more comprehensive picture of the issue being researched. With this methodological approach, this research is expected to be able to make a significant contribution to the development of regulations and law enforcement practices in Indonesia, especially in the context of the use of surveillance technology in the investigation of cybercrimes.

RESULTS AND DISCUSSION

The use of surveillance technology in the investigation process of cyber crimes in Indonesia shows significant developments in law enforcement efforts in the digital era. Based on a juridical analysis of existing laws and regulations, it can be seen that surveillance technologies such as network monitoring, surveillance software, and big data analysis have been recognized as legitimate tools in the investigation process. However, the application of this technology still faces various challenges, especially related to privacy issues and the legality of the evidence obtained. In some cases, the use of surveillance technology has caused controversy because it is considered to violate the privacy rights of individuals guaranteed by the constitution (Darmawan, 2023).

One of the main issues faced in the use of surveillance technology is the limitations of existing regulations. Although several regulations have regulated the use of technology in criminal investigations, there are still significant legal gaps. Existing regulations have not specifically regulated the limits and procedures that law enforcement must follow in using surveillance technology. This leads to the potential for misuse of technology, where law enforcement may violate the basic rights of individuals without clear sanctions. Therefore, there is an urgent need to develop more comprehensive and detailed regulations (Echa & Shalauddin, 2024).

The legal implications of the use of surveillance technology are also seen in terms of the receipt of evidence in court. In Indonesia's criminal justice system, the evidence obtained must meet certain conditions in order to be accepted at trial. However, in practice, there is uncertainty regarding the legality of evidence obtained through surveillance technology. Some court rulings show that evidence obtained in a way that violates legal procedures is not always admissible, even though the technology used is very effective in uncovering cybercrimes. This poses a dilemma for law enforcement, where they must choose between adhering to strict legal procedures or using more advanced technology but risking being rejected in court (Suriyani et al., 2023).

Analysis of court decisions also shows variations in the application of laws related to surveillance technology. Some courts tend to be stricter in assessing the legality of evidence, while others are more flexible in accepting evidence obtained through modern technology. This inconsistency reflects ambiguity in existing regulations, as well as the need for clearer guidance for judges in assessing evidence obtained through surveillance technology. In addition, these inconsistencies can also reduce legal certainty, which is a basic principle in the judicial system (Arief & Ambarsari, 2018).

In the operational context, the use of surveillance technology also poses its own challenges for law enforcement. While this technology offers various advantages in terms of efficiency and effectiveness, its application in the field requires adequate skills and knowledge. The study found that most investigators in Indonesia still need additional training to be able to use surveillance technology optimally. Without adequate training, there is a risk that the technology will not be used effectively, or may even be misused, ultimately harming the investigation process (Hakim, 2014).

Interviews with legal practitioners revealed that one of the biggest obstacles to the use of surveillance technology is resistance to change. Some law enforcement is still reluctant to use new technology due to a lack of understanding or discomfort with complex technological devices. This hampers modernization efforts in law enforcement and reduces the potential of surveillance technology to detect and prevent cybercrime more effectively. Therefore, a cultural change is needed among law enforcement to accept and adopt technology as part of a legitimate law enforcement tool (Simatupang & Nofrial, n.d.).

In addition, this study also shows that there is a need to strengthen cooperation between various law enforcement agencies in the use of surveillance technology. In some cases, the lack of coordination between institutions has resulted in overlap in the use of technology or even conflicts of authority. Closer cooperation is needed to ensure that surveillance technology is used effectively and efficiently, as well as to avoid abuse of authority. With good coordination, law enforcement can maximize the potential of technology in eradicating cybercrime (Purba & Mauluddin, 2023).

In the juridical analysis, it is important to note that existing regulations not only need to pay attention to the technical aspects, but must also consider the social and ethical impacts of the use of surveillance technology. The use of these technologies, if not properly regulated, can raise concerns in society related to excessive surveillance or misuse of personal data. Therefore, the development of regulations must involve various stakeholders, including civil society, to ensure that the basic rights of citizens are still protected (Dasyah & Desiandri, 2023).

Finally, this study highlights the importance of regular legal updates to adapt to rapid technological developments. Surveillance technology is constantly evolving and will always present new challenges for law enforcement and the justice system. Therefore, existing regulations must be updated regularly to ensure that the law remains relevant and effective in facing future challenges. This legal update must also be accompanied by continuous education and training for law enforcers, so that they are always ready to face dynamic technological developments (Rizki, 2022).

CONCLUSION

The importance of the role of surveillance technology in the investigation process of cyber crimes in Indonesia. Surveillance technology has proven to be a highly effective tool in uncovering and analyzing complex cybercrimes. However, this effectiveness must be balanced with strict and specific regulations so that the use of technology does not violate human rights, especially related to privacy and individual freedom. With clear regulations, surveillance technology can be optimized in the investigation process without sacrificing the principles of justice and legal certainty (Swantoro et al., 2017).

Furthermore, law enforcement in Indonesia still needs to increase capacity in terms of knowledge and skills to operate surveillance technology effectively. Ongoing training and improved coordination between law enforcement agencies are essential to ensure that these technologies are used appropriately and in accordance with applicable legal standards. In addition, cultural changes among law enforcement are also needed to overcome resistance to new technologies, so that modernization in law enforcement can run more smoothly and effectively (Rumangun et al., 2023).

Finally, regulations governing the use of surveillance technology must be constantly updated in line with the rapid development of technology. These updates must involve a wide range of stakeholders, including civil society, to ensure that applicable laws remain relevant and able to address future challenges. With dynamic regulations and adaptive law enforcement, Indonesia can better meet the challenges of cybercrime, while effectively protecting the basic rights of its citizens.

REFERENCES

Arief, H., & Ambarsari, N. (2018). Penerapan Prinsip Restorative Justice Dalam Sistem Peradilan Pidana Di Indonesia. *Al-Adl: Jurnal Hukum*, *10*(2), 173–190.

Bambang, S., Setyadji, S., & Darmawan, A. (2021). Penanganan tindak pidana pemilu dalam sentra penegakkan hukum terpadu (Gakkumdu). *Jurnal Indonesia Sosial Teknologi*, *2*(02), 281–291.

Darmawan, S. P. (2023). *Hak Konstitusional Atas Privasi di Era Digital*.

Dasyah, F., & Desiandri, Y. S. (2023). Integrasi Nilai Hak Asasi Manusia dalam Proses Pemilihan Umum di Indonesia. *Jurnal Pendidikan Tambusai*, *7*(3), 29156–29161.

Echa, A. N., & Shalauddin, Y. (2024). Perbedaan Tata Kelola Audit Syariah Di Indonesia Dan Malaysia: Analisis Terhadap Praktik Dan Regulasi Audit Syariah (Studi Literatur Di Indonesia Dan Malaysia). *Accounting Research Journal*, *2*(2), 102–111.

Flora, H. S., SH, M., Kn, M., Kes, M. H., Kasmanto Rinaldi, S. H., SI, M., Jusri Mudjrimin, S. H., Sitta Saraya, S. H., Yusrina Handayani, S. H., & Ratna Jaya, S. H. (2024). *Hukum Pidana di Era Digital*. CV Rey Media Grafika.

Hakim, U. (2014). Eksistensi akuntansi forensik dalam penyidikan dan pembuktian pidana korupsi. *Unnes Law Journal*, *3*(1).

Lestari, A. D., & Damayanti, M. (2018). Cakupan Alat Bukti Sebagai Upaya Pemberantasan Kejahatan Siber. *Al-Ahkam: Jurnal Ilmu Syari'ah Dan Hukum*, *3*(1), 47–68.

Malau, P. (2023). Tinjauan Kitab Undang-Undang Hukum Pidana (KUHP) Baru 2023. *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam*, *5*(1), 837–844.

Purba, Y. O., & Mauluddin, A. (2023). Kejahatan Siber dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi Tentang Potensi Pencurian Data Online. *JCIC: Jurnal CIC Lembaga Riset Dan Konsultan Sosial*, *5*(2), 55–66.

Rizki, M. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi:-. *Politeia: Jurnal Ilmu Politik*, *14*(1), 54–62.

Rumangun, J. P. E., Uktolseja, N., Arloy, W., & Lawalatta, M. (2023). Kebijakan Penegakan Hukum Pidana Pada Wilayah Pulau-Pulau Kecil Perbatasan di Kabupaten Kepulauan Aru. *Jurnal Pendidikan Tambusai*, *7*(3), 20021–20028.

Sianipar, S. P. F., & Sembiring, T. B. (2024). Peran Saksi Ahli Dalam Proses Peradilan Pidana Perspektif Hukum Dan Etika. *Journal of International Multidisciplinary Research*, *2*(1), 242–255.

Simatupang, H. S. R. E. B., & Nofrial, R. (n.d.). *Analisis Yuridis Penggunaan Informasi/Dokumen Elektronik Sebagai Alat Bukti Dalam Penegakan Hukum Pidana (Studi Perkara Putusan Nomor: 192/Pid. B/2023/PN Btm)*.

Soraja, A. (2021). Perlindungan Hukum Atas Hak Privasi Dan Data Pribadi Dalam Prespektif HAM. *Seminar Nasional-Kota Ramah Hak Asasi Manusia*, *1*, 20–32.

Suriyani, H., Suryanti, N., & Kusmayanti, H. (2023). Perlindungan Hukum Bagi Anak Pasca Putusan Dispensasi Kawin yang Ditolak Berdasarkan Peraturan Perundang-Undangan Terkait. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *1*(4), 302–316.

Swantoro, H., Fakhriah, E. L., & Ikhwansyah, I. (2017). Permohonan upaya hukum peninjauan kembali kedua kali berbasis keadilan dan kepastian hukum. *Mimbar Hukum-Fakultas Hukum Universitas Gadjah Mada*, *29*(2), 189–204.

Syam, A. P., Mahrus, M. M. P., & Tarigan, T. M. (2023). Peran Etika Profesi Hukum sebagai Upaya Penegakan Hukum. *As-Syar'i: Jurnal Bimbingan & Konseling Keluarga*, *5*(2), 462–470.