THE LEGAL AND ETHICAL IMPLICATIONS OF SURVEILLANCE IN CRIMINAL LAW: A LITERATUR REVIEW

Andi Cakra Cindrapole[1]*, Siti Rosmini[2]
[1,2] Fakultas Hukum, Universitas Muslim Indonesia, Indonesia
*) corresponding author: andicakra.cindrapole@umi.ac.id

Keywords

Surveillance in criminal law; Data privacy and criminal law; Literature Review

Abstract

This study investigates the legal and ethical implications of the use of surveillance technology in criminal law through a comprehensive literature review. With the increasing capacity of technologies such as CCTV, digital surveillance, and the use of big data, important questions arise regarding the balance between security and personal rights. The study analyzes a variety of sources from journal articles, court rulings, and policy documents to identify key issues faced by legal practitioners and policymakers. The results of this review show that there is an intense debate between the need for security and the protection of individual privacy. The study also explores how different jurisdictions are responding to these challenges and proposes a framework to ensure that the use of surveillance technology remains accountable and transparent. This literature review aims to provide in-depth insight into the emerging complexities at the intersection of technology, ethics, and criminal law, while offering guidance for legal professionals in formulating ethical and effective strategies for addressing crime.

1. INTRODUCTION

Surveillance has become a very important tool in the context of criminal law enforcement, especially with the rapid development of technology(Uddin, 2022). Basically, surveillance refers to surveillance carried out by authorities to monitor the activities of certain individuals or groups with the aim of gathering useful information in the prevention, investigation, and prosecution of criminal acts (Fissell, 2018). Surveillance can take the form of various methods, ranging from the use of CCTV cameras in public spaces, phone tapping, to monitoring digital activities on the internet. The use of this technology allows law enforcement to more effectively identify and crack down on criminals, as well as provide additional security to the community. With the ability to collect data at scale and in real-time, surveillance plays a crucial role in tackling various forms of crime, including terrorism, cybercrime, and narcotics trafficking (Brayne, 2014).However, the application of surveillance in criminal law also raises various legal and ethical questions. One of the main issues that has emerged is how to balance the need to maintain public safety with the legally recognized privacy rights of individuals (Turillazzi et al., 2023). Excessive or indefinite surveillance can lead to privacy violations, abuse of power, and discrimination (Fissell, 2018). On the other hand, a lack of oversight can make the law lose an effective tool to protect society from the threat of crime. Therefore, it is important to have a clear and transparent legal framework that governs the use of surveillance by law enforcement authorities, ensuring that the practice is carried out lawfully, proportionately, and in accordance with human rights principles (Choudhary, 2024)

The use of digital surveillance has also increased in line with the development of the internet and information technology. The digital footprint generated from online activities, such as social media use, internet searches, and electronic financial transactions, provides a new source of information that law enforcement can leverage to identify and track criminal activity (Lyon, 2014). Specialized software and big data analytics tools allow law enforcement to extract patterns and trends from the collected digital data, which can be used to detect potential threats or suspicious behavior. For example, with digital wiretapping technology and monitoring of communication networks, authorities can monitor electronic conversations to prevent terrorist attacks or uncover organized crime networks.

However, while advanced surveillance technology offers great benefits in the areas of security and law enforcement, its increased use also raises significant concerns regarding individual privacy and freedom. Technologies that enable mass surveillance and non-consensual data collection pose a risk of abuse and human rights violations (Čehulić, 2021). The pace of technological development often outpaces the speed of regulation, which means that many new forms of surveillance operate within unclear or even non-existent legal frameworks. Therefore, a careful and measured approach is needed in implementing surveillance technology, ensuring that its use is equipped with appropriate regulations, transparency, and oversight mechanisms to prevent abuse and maintain a balance between security and civil rights (Lyon, 2014).

In today's digital era, legal and ethical issues related to surveillance are becoming increasingly important in the context of criminal law due to the increasingly widespread and sophisticated use of surveillance technology. With technological advancements such as facial recognition, GPS-based surveillance, and big data analytics, law enforcement now has the ability to conduct more in-depth and thorough surveillance than ever before (Laufs & Borrion, 2022). While this can increase effectiveness in detecting and preventing crime, it can also threaten individual privacy rights. Law enforcement that relies too heavily on surveillance can easily violate legally protected privacy rights, which can lead to human rights violations and abuse of power. Therefore, legal issues that limit the extent to which surveillance can be used as well as how the data collected is managed and protected are of paramount importance (Čehulić, 2021).

In addition to legal issues, ethical considerations are also crucial because surveillance concerns the supervision of an individual's personal life. Poorly regulated surveillance can create feelings of being watched and violate civil liberties, which in turn can undermine public trust in law enforcement and government (Molldrem & Smith, 2020). An ethical dilemma arises when efforts to improve security through surveillance must be balanced with the protection of individual freedoms. For example, is the application of invasive surveillance technology justified in the context of preventing crime, or will it create a society that is always under surveillance? These issues require in-depth debate and clear policies to ensure that surveillance practices are implemented proportionately and transparently, taking into account their long-term impact on individual rights and democracy (Barabas, 2019).

Research by Lyon (2018) investigated how surveillance technology has changed and evolved along with digital advancements, showing that big data-driven surveillance is

becoming an important tool in modern law enforcement. Lyon emphasized that, while this technology can improve efficiency in identifying and tracking criminals, it also underscores potential risks to individual privacy and potential human rights violations. This study shows that clear and comprehensive regulations are urgently needed to limit the use of surveillance and protect civil liberties. research by Zarsky (2016) focuses on the ethical dilemmas faced in the application of surveillance technology. Zarsky discusses the concept of a "chilling effect" in which individuals change their behavior because they feel constantly watched, which can limit freedom of expression and reduce active participation in society. The study emphasizes that a balance between public safety and privacy rights must always be maintained. Zarsky's research also highlights the importance of informed consent and transparency in the collection and use of data obtained through surveillance. In other words, the public should be informed about how their data is monitored and used, and there are oversight mechanisms in place to ensure that surveillance technology is not misused.

2. RESEARCH METHODS

This study uses a systematic literature review approach to examine the legal and ethical implications of the use of surveillance in criminal law. This method involves identifying, selecting, and critically analyzing relevant literature, which includes academic journal articles, books, legal reports, and case studies that address surveillance, criminal law, privacy, and ethics. Literature searches were conducted through academic databases such as JSTOR, Google Scholar, and ProQuest using specific keywords, such as "surveillance in criminal law," "legal implications of surveillance," and "ethical issues in surveillance." Inclusion criteria for selected literature include relevance to the research topic, published in the last five to ten years, as well as literature that provides a comprehensive perspective on legal and ethical aspects.

Once the relevant literature has been identified, the next step is to conduct data analysis and synthesis to identify key themes and gaps in the existing research. This approach allows researchers to build a deep understanding of the issues raised and how they have been discussed in the context of criminal law. The analysis is conducted by evaluating the arguments and findings of previous research, identifying patterns and trends, and highlighting areas where debate is still ongoing or where further research is needed. Through this literature review method, the research aims to provide a comprehensive and critical understanding of the legal and ethical implications of surveillance, as well as provide recommendations for future policy and regulatory development.

3. RESULT AND DISCUSSION

3.1 Surveillance in Criminal Law

Surveillance in criminal law has become an increasingly vital component of law enforcement efforts around the world. With increasingly advanced technology, law enforcement now has access to a variety of sophisticated surveillance tools, from CCTV cameras, digital surveillance, to facial recognition devices that can be used to monitor the activities of the public and individuals more effectively. The main purpose of using surveillance

in this context is to prevent criminal acts, identify perpetrators of crimes, and gather relevant evidence for prosecution. In many countries, surveillance has proven effective in lowering crime rates and improving responses to security threats (Molldrem & Smith, 2020).

However, while the benefits are clear, the use of surveillance in criminal law also raises a range of complex legal and ethical issues. One of the main issues is the potential for individual privacy violations. Surveillance technology capable of monitoring people's daily activities in detail can easily violate the privacy rights protected by the constitution and international law (Alikhademi et al., 2022). The question that arises is to what extent states can collect and use personal information without the explicit consent of the individuals being supervised. Court cases in various jurisdictions often dispute the boundaries between the right of states to ensure security and the individual's right to privacy.

In addition, surveillance can raise concerns about discrimination and profiling. Facial recognition technologies and algorithms used in surveillance often have unconscious biases that can lead to discrimination against minorities or other vulnerable groups. For example, studies have shown that facial recognition devices are more likely to misidentify individuals from racial minorities compared to individuals from majority groups (Choudhary, 2024). This not only raises legal but also ethical problems, as it can lead to unfair law enforcement and reinforce social prejudices.

From a legal standpoint, the regulatory framework for regulating the use of surveillance in criminal law differs from country to country and is often not uniform. Some countries have comprehensive laws that govern how data collected through surveillance can be used and stored, as well as establish standards of transparency and accountability (Turillazzi et al., 2023). However, many other countries have not developed adequate legal frameworks, leading to the use of surveillance that is poorly regulated and potentially violates human rights. These differences point to the need for more consistent international standards to protect privacy and civil liberties while enabling the use of surveillance for security purposes.

Surveillance in criminal law also raises ethical questions about mass surveillance versus targeted surveillance. While mass surveillance can provide extensive information and potentially prevent major attacks, the practice is often criticized for its lack of focus and potential for misuse of personal data on a large scale. In contrast, targeted surveillance, which focuses on suspected individuals or groups, is considered more respectful of privacy, but requires stronger evidence to be implemented. Law enforcement needs to find a balance between the effectiveness of surveillance and the protection of individual rights, ensuring that surveillance is used proportionately and fairly (Meskys et al., 2020)

Finally, the importance of supervision and transparency in the use of surveillance cannot be ignored. External oversight mechanisms, such as specialized courts or independent agencies, can serve to ensure that the use of surveillance by law enforcement is in line with the law and ethical principles. Without adequate oversight, there is a risk that surveillance technology could be misused for purposes outside of law enforcement, such as monitoring political activities or intimidating political opponents. As such, transparency in surveillance operations and clear accountability are key to maintaining public trust and ensuring that individual rights are respected.

Overall, surveillance in criminal law is a powerful tool that can provide great benefits in maintaining security and order. However, to harness its full potential, its use must be accompanied by strict regulation, transparent oversight, and serious attention to legal and ethical implications. Thus, law enforcement can achieve security objectives without sacrificing fundamental freedoms and human rights.

3.2 Ethics Related to Surveillance in Criminal Law

Ethics related to surveillance in criminal law are becoming an increasingly important topic in the digital era, where surveillance technology has become an integral part of law enforcement efforts. The main ethical question that arises is the extent to which the right of the state to monitor and collect information about its citizens in the interest of security can be justified (Laufs & Borrion, 2022). The basic principle of ethics in this context is a balance between the need to protect society from criminal threats and the obligation to respect the privacy rights of individuals. Surveillance, if used inappropriately, can violate privacy, restrict individual freedom, and create fear or mistrust among the public (Charbonneau & Doberstein, 2020).

One of the prominent ethical issues is the potential misuse of data collected through surveillance. The personal information obtained may be used for purposes outside of law enforcement, such as monitoring legitimate political or social activity, which could lead to intimidation or discrimination. Surveillance ethics demand that the data collected be used only for legitimate, proportionate, and necessary purposes, and that it is protected with strong security mechanisms to prevent unauthorized access. Transparency in the process of collecting and using data is also important to ensure that individuals understand their rights and the purpose for which the data was collected (Charbonneau & Doberstein, 2020).

Another ethical issue is the problem of bias and discrimination in the application of surveillance technology. The algorithms and facial recognition systems used often show bias against certain minority or ethnic groups, which can lead to misidentification and unfair law enforcement. This poses an ethical dilemma because biased law enforcement can exacerbate social inequalities and undermine public trust in the justice system(Laufs & Borrion, 2022). Law enforcement must ensure that the surveillance technology used is free of discriminatory bias and that corrective measures are in place to address possible errors.

In addition, there are ethical questions related to mass surveillance versus targeted surveillance. Mass surveillance, which includes the collection of data at scale without discrimination, is often considered to violate an individual's right to privacy because it is not based on special suspicions. Law enforcement ethics require that surveillance be conducted in the least invasive manner, and only when there is a compelling reason to suspect that a particular individual or group is involved in criminal activity. Targeted surveillance is more aligned with ethical principles because it respects individual rights more and reduces the risk of human rights violations.

Ethical oversight in the use of surveillance also involves the importance of informed consent and the right to know. Individuals have the right to know if and how they are supervised, as well as how their information is used and stored. It emphasizes the need for

clear regulations governing surveillance practices, as well as the need for independent oversight bodies to ensure that law enforcement acts in accordance with the law and ethical standards. These external oversight mechanisms are important to prevent abuse of power and ensure that surveillance is used responsibly (Shachar et al., 2020).

Finally, ethical issues in surveillance also include their impact on society as a whole. When individuals feel constantly watched, this can create a chilling effect where people may refrain from participating in public activities, speaking freely, or engaging in legitimate activities for fear of surveillance (Fissell, 2018). This can undermine democratic values such as freedom of expression and freedom of assembly. Therefore, law enforcement must consider the long-term impact of surveillance practices on civil and social rights and ensure that their approach does not undermine the foundations of democracy and individual freedoms.

Taking these ethical issues into account, it is important for law enforcement and policymakers to design and implement surveillance policies that are consistent with ethical and human rights principles. This includes ensuring that surveillance is carried out in proportion, necessary for security, transparency, and well-supervised to prevent abuse and protect public confidence in legal institutions (Ejjami, 2024).

3.3 The Impact of Surveillance on Public Trust

Surveillance, while intended to improve public safety and prevent crime, can have a significant impact on public trust in law enforcement institutions and governments. The existence of extensive surveillance technologies, such as CCTV cameras, facial recognition, and digital monitoring, can create a feeling of constant surveillance among the public. This can affect the way people view their personal freedoms and create concerns about the potential misuse of personal information (Choudhary, 2024). If the public feels that their privacy is not respected or that information collected through surveillance is being used in an untransparent or unauthorized manner, this can lead to an erosion of trust in law enforcement and government agencies (Shachar et al., 2020).

The lack of transparency in surveillance operations can exacerbate this trust problem. When people are not clearly informed about how, when, and why they are being monitored, or if there is an impression that surveillance is being done in secret (Freilich et al., 2024), a sense of distrust can increase. Ambiguity regarding the use of the data collected, including how it is stored, who has access to it, and how it is used, can also be a cause for concern. Public trust requires confidence that law enforcement not only protects security but also respects individual rights and is transparent in its operations.

The chilling effect is another impact of surveillance that can damage public trust. When individuals feel watched, they may become more reluctant to engage in social, political, or freedom of expression activities, which can reduce public participation and open dialogue. The feeling that every action or speech is being watched can significantly change people's behavior, causing them to become more introverted or obedient for fear of surveillance. It can inhibit creativity, intellectual freedom, and the diversity of views that are the foundation of a healthy and democratic society (Benneh Mensah, 2023).

In addition, surveillance that is too extensive or not targeted can create the perception that the government is intrusive and considers all citizens as potential suspects (Molldrem & Smith, 2020). This can exacerbate tensions between society and law enforcement, especially in communities that feel that they are being monitored more closely or unfairly profiled based on race, ethnicity, or socioeconomic background. When certain segments of society feel intimidated or treated unfairly by surveillance technology, this can reinforce existing feelings of marginalization and mistrust, deepening the gap between law enforcement and society.

Conclusion

The results of this study highlight that surveillance in criminal law has significant legal and ethical implications, which require serious attention from policymakers, law enforcement, and the public. While surveillance can increase the effectiveness of law enforcement in preventing and tackling crime, its widespread and sophisticated use also carries the risk of privacy violations, discrimination, and abuse of power. This research shows that a careful balance between the need to maintain public safety and the protection of individual rights is essential. To achieve this balance, a clear legal framework, transparency in surveillance operations, and strong oversight mechanisms are needed to prevent abuse.

REFERENCE

Alikhademi, K., Drobina, E., Prioleau, D., Richardson, B., Purves, D., & Gilbert, J. E. (2022). A review of predictive policing from the perspective of fairness. *Artificial Intelligence and Law*, *30*(1), 1–17. https://doi.org/10.1007/s10506-021-09286-4

Barabas, C. (2019). Beyond Bias: Re-Imagining the Terms of 'Ethical AI' in Criminal Law. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3377921

Benneh Mensah, G. (2023). *Regulations and Guidelines for AI Health Apps*. https://doi.org/10.13140/RG.2.2.35112.17925

Brayne, S. (2014). Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment. *American Sociological Review*, *79*(3), 367–391. https://doi.org/10.1177/0003122414530398

Čehulić, M. (2021). Perspectives of Legal Culture: A Systematic Literature Review. *Revija Za Sociologiju*, *51*(2), 257–282. https://doi.org/10.5613/rzs.51.2.4

Charbonneau, É., & Doberstein, C. (2020). An Empirical Assessment of the Intrusiveness and Reasonableness of Emerging Work Surveillance Technologies in the Public Sector. *Public Administration Review*, *80*(5), 780–791. https://doi.org/10.1111/puar.13278

Choudhary, V. (2024). *AI in Crime Prediction and Prevention*. https://doi.org/10.13140/RG.2.2.22509.60642

Ejjami, R. (2024). AI-Driven Smart Cities in France. *International Journal For Multidisciplinary Research*, *6*. https://doi.org/10.36948/ijfmr.2024.v06i03.21920

Fissell, B. (2018). Nondelegation and Criminal Law. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3258618

Freilich, J. D., Chermak, S. M., Arietti, R. A., & Turner, N. D. (2024). Terrorism, Political Extremism, and Crime and Criminal Justice. *Annual Review of Criminology*, *7*(1), 187–209. https://doi.org/10.1146/annurev-criminol-022422-121713

Laufs, J., & Borrion, H. (2022). Technological innovation in policing and crime prevention: Practitioner perspectives from London. *International Journal of Police Science & Management*, *24*(2), 190–209. https://doi.org/10.1177/14613557211064053

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 2053951714541861. https://doi.org/10.1177/2053951714541861

Meskys, E., Liaudanskas, A., Kalpokiene, J., & Jurcys, P. (2020). Regulating deep fakes: Legal and ethical considerations. *Journal of Intellectual Property Law & Practice*, *15*, 24–31. https://doi.org/10.1093/jiplp/jpz167

Molldrem, S., & Smith, A. K. J. (2020). Reassessing the Ethics of Molecular HIV Surveillance in the Era of Cluster Detection and Response: Toward HIV Data Justice. *The American Journal of Bioethics*, *20*(10), 10–23. https://doi.org/10.1080/15265161.2020.1806373

Shachar, C., Gerke, S., & Adashi, E. Y. (2020). AI Surveillance during Pandemics: Ethical Implementation Imperatives. *Hastings Center Report*, *50*(3), 18–21. https://doi.org/10.1002/hast.1125

Turillazzi, A., Taddeo, M., Floridi, L., & Casolari, F. (2023). The digital services act: An analysis of its ethical, legal, and social implications. *Law, Innovation and Technology*, *15*(1), 83–106. https://doi.org/10.1080/17579961.2023.2184136

Uddin, M. (2022). *Legal and Ethical Aspects of Deploying Artificial Intelligence in Climate-Smart Agriculture (AI & Society) (Springer)*.