Chapter 18
Ethical Considerations in Drone Surveillance

Revanth Madamala
TikTok, Bytedance Pvt. Ltd., USA

Naga Lalitha Sree Thatavarthi
Srisan Group Inc, USA

Raviteja Reddy Ganta
TikTok, Bytedance Pvt. Ltd., USA

M. Nagabhushan Rao
https://orcid.org/0000-0003-3544-3031
Malla Reddy University, Hyderabad, India

M. Rajeshwari
Presidency University, Bangalore, India

ABSTRACT

Blockchain and IoT are strongly impacting how security is being handled using drones. With blockchain and IoT technology in drones, surveillance operations are safer and more trusted. The use of drones is becoming more common which is raising some ethical issues, especially about privacy, security and taking responsibility. This addresses how these main subjects deal with the challenge of keeping people protected and allowing them their rights. It analyzes drone usage in surveillance and studies the privacy concerns and the possibility of bad use of gathered information. Also, it takes care of legal matters regarding such systems, especially with data protection and accountability when using drones. Since drones work on their own, the report states that it is still tough to put guidelines in place that stop misuse. It covers the important issues in using blockchain, the Internet of Things and drones for surveillance and offers approaches to deal with these issues and gain the benefits of their use.

DOI: 10.4018/979-8-3373-4277-1.ch018

1. INTRODUCTION

Surveillance by drones has become a leading technology used in security in different fields, for example, law enforcement, disaster control, the environment and infrastructure. With drones equipped with high-tech equipment, large regions can be watched continuously which means responses to emergencies can be rapid. Because of this, surveillance can now be done more effectively and cover a wider area. Before drones existed, security was mainly done in one place, but drones allow flexible coverage of both remote and crowded areas, much quicker than traditional methods. Joining blockchain, IoT and drones has taken the power of surveillance systems to an entirely different level. Thanks to IoT, drones can always collect and share information such as environmental readings and video footage which supports early and flexible security actions. Blockchain technology improves these systems by making it safe and clear where all the data is stored. Information collected using blockchain is protected against modifications and is trackable, because blockchain's decentralized nature. Due to these improvements, drones can carry out sophisticated surveillance work on their own which is crucial for the modern security industry (Lenhard et al., 2024).

Because drone technology is developing and growing, there are many new ethical issues that shouldn't be ignored. Blockchain and IoT are excellent security tools, but they also bring up big concerns about privacy, data protection and responsibility. Drones are able to collect a lot of information and this frequently consists of private or confidential data. Also, this may cover scenes inside private homes or ways a person behaves that could be easily misused. Because drones can work without much human involvement, these issues about privacy are more complicated. The biggest ethical concern with drone surveillance is about privacy. As drones become more useful for advanced surveillance, people's privacy is harder to define. Drones are used to watch individuals in crowds as well as in private areas, getting information on people's movements, talk and what they do. There is a risk that this information could be used either without consent or not as intended which may threaten individual privacy (Laroca et al., 2025).

Security of data ranks high along with issues about privacy. Surveillance data may cover confidential information about individuals or about the environment. Because drones produce so much data, they may be vulnerable to hacking, data loss or access by unauthorized people. Keeping drone surveillance systems ethical means that securing their information is very important. Blockchain technology could help ease the problem of ensuring data transparency. Blockchain makes data security stronger by storing information in an immutable and decentralized way, so once the data is on the ledger, it cannot be altered. Because blockchain makes everything transparent, it becomes clear who accesses the data and where it is coming from which helps prevent the misuse of information collected for surveillance. The decision about managing drones is another ethical challenge, mainly when these systems can act independently. With new updates, many drones can decide what to do by themselves, following instructions they've been given. There are major worries about responsibility with this system. Who has responsibility when an autonomous drone infringes someone's privacy or causes harm? Is responsibility for checking cybersecurity with the operator, manufacturing company or the team that built the software? Drones can make decisions independently which sometimes goes against ethical and legal rules. Because of this, there should be set rules that explain who is responsible for drones and how they can be programmed to obey laws and ethical standards (Wang et al., 2024).

Likewise, using drones without any human control could allow the technology to be used improperly. Even though drones support surveillance, they may also be used to spy on people or target individuals unfairly. Automated systems in drones may end up spreading biases or could be used to discriminate against