UDC 004.8:174.9

THE PROBLEM OF EXCESSIVE SURVEILLANCE: ETHICAL RISKS OF INTRODUCING COMPUTER VISION INTO ROBOTICS

Khaniak Y. D., student
Belarusian National Technical University
Minsk, Republic of Belarus
Scientific supervisor: trainee teacher Shukalo M. S.

Abstract. This article is about the ethical problems that appear when service robots with computer vision become common in public and private human spaces. They collect large amounts of personal data, while people have almost no control over this process. The topic argues that the closed model of development creates a deep crisis of trust, because it makes transparency and verification impossible.

The blitz development of service robots and technologies in recent years has changed usual human environments visibly. Robots now work as drivers in taxi, deliver food on the streets, transport objects in storages, and perform other routine tasks. Many of them use computer vision to recognize objects, detect people, and create detailed maps of the spaces where they operate. This technology allows robots to complete tasks efficiently, but it also means that robots constantly observe human behavior and collect information about private spaces, often without direct interaction or permission from the individuals present. Modern society faces a new ethical challenge: people do not fully understand what data robots collect, how long it is stored, or for what purposes it may be used [1].

The core of the problem is the huge difference of information and power between robot producers and the people who live or work near them. A company receives a flow of intimate and sensitive data through its machines. At the same time, ordinary users cannot check the robot's software, see what information is transferred to servers, or know whether these data are later sold, analyzed, or used in ways that were never explained. Even when companies claim they protect privacy, users have no way to verify these statements. Privacy becomes a matter of trust rather than a proven technical guarantee, and trust alone is not a reasonable ethical foundation when technologies operate inside personal living spaces.

This problem becomes clearer in comparison with technologies that people already understand – web browsers, for example. Browsers also collect user data, but their data practices are documented, visible, and can be controlled through settings, extensions, and independent audits. Users can disable cookies, block tracking scripts, delete browsing history, or switch to open-source browsers whose code can be inspected publicly. Most importantly, the user initiates the interaction. With service robots, none of these mechanisms exist. Their cameras operate continuously, their data flows are invisible, and the user cannot simply "turn off" the robot's analytics. Robots collect more intimate spatial information in an environment with much lower transparency.

For this reason, the closed model of robot development is an ethical problem by itself. Internal processes are hidden from independent experts. Algorithms that analyze images and store data cannot be inspected, and the real behavior of the machine cannot be confirmed by outside specialists. Even if a company has honest intentions, the structure of the system does not allow society to confirm this honesty. The inability to verify claims about safety and privacy creates a long-term crisis of confidence. People may accept robots in their environment, but they do so without real choice and without understanding the risks they carry.

This situation becomes more serious because many interactions with service robots are not voluntary. People in public or shared spaces cannot easily avoid a robot that records the environment while doing its tasks. A person walking past a delivery robot does not choose to

take part in that data collection. Consent is symbolic, and individuals lose real control over what information is gathered and how it might be used.

If robots continue to be developed as closed systems, this imbalance will grow. Trust between society and technology will decrease, and companies may face pressure from regulators. Strict rules may appear, which can slow down innovation. Because robots operate in real physical spaces and collect continuous visual information, the risks of misuse or misunderstanding are higher than in many other digital technologies.

To reduce these risks, robot design needs new technical and institutional solutions that increase transparency and provide real protection. One promising approach is to build robots around a standardized and limited communication interface [2]. The robot's "brain" receives data only through a clear and predictable API. The computer vision module works independently and processes raw images internally. It never sends full images to the robot but communicates only through the certified API, transmitting simple metadata, such as obstacle positions or recognized object categories. The public and standardized API allows experts to verify what information the robot can receive and what it cannot.

This design allows the insertion of a filtering module between the computer vision subsystem and the robot's controller. The filter removes sensitive information before it reaches the robot's "brain" and is enforced by hardware. If the computer vision subsystem cannot physically send unprocessed images, a software update cannot bypass protection. This technical barrier makes privacy a built-in property of the robot, not just a company promise.

The system only works if the manufacturer cannot create a hidden alternative channel. The CV module must have exactly one physical output, which complies with the standardized API. The filter must sit directly on this line, and the CV subsystem should have no wireless interfaces, hidden storage, or extra communication ports. The robot is then limited to receiving only the safe and predefined data types allowed by the certified API.

National regulators could certify the filtering module and verify that the CV subsystem has no additional channels. Certification of the entire data path – from camera to final metadata – allows independent experts to check privacy compliance. Any update to the CV software or filtering logic would require new certification, preventing silent changes in data practices.

This approach has disadvantages. Separation of modules makes robots more complex and expensive to produce, and certification increases development time. Companies may need to redesign hardware and follow new standards. Regulators require resources to evaluate these systems. But these costs are justified, because the result is a robot whose behavior can be verified both in theory and in practice.

In conclusion, ethical use of service robots with computer vision cannot rely only on developer promises. When robots operate in human spaces and collect large amounts of data, society needs real, verifiable guarantees. A standardized API between the CV module and the robot's "brain," combined with hardware-enforced filtering and mandatory certification, creates a system in which privacy is protected by design. Robots become safer, more transparent, and easier for people to accept. Privacy becomes a guaranteed element of the robot's architecture, not just a declaration in documentation.

References

1. Lin, P. Robot Ethics: The Ethical and Social Implications of Robotics / P. Lin, K. Abney, G. A. Bekey. – Cambridge, MA: MIT Press, 2011. – 400 p.

2. Calo, M. R. Robots and Privacy // Robot Ethics: The Ethical and Social Implications of Robotics. Cambridge. – MA: MIT Press, 2011. – P. 187–202.