OPEN DATA, DATA MINING AND PERSONAL DATA IN LAW ENFORCEMENT ENVIRONMENT

Mišo Mudrić[1]

[1] Faculty of Law, University of Zagreb, Croatia

*correspondence E-mail: miso.mudric@pravo.hr

Keywords: Facial recognition; Law enforcement bodies; LED Directive; Draft EU AI Act; CCTV surveillance

In recent years, the law enforcement bodies have increasingly begun to use the facial recognition technology as a tool for identifying suspects and solving crimes. This technology is based on the use of algorithms that can analyze and match facial features to a database of known individuals. One of the main advantages of using facial recognition technology is that it can help to identify suspects quickly and accurately. This can be especially useful in cases where traditional methods of identification, such as fingerprint analysis or DNA testing, are not available or are not effective. Facial recognition technology can be used to monitor large crowds, such as at public events or in high-crime areas, to identify potential suspects or persons of interest. Another benefit of using facial recognition technology is that it can help to reduce the number of false arrests and wrongful convictions. This is because the technology is based on objective criteria and is not subject to human bias or error. Additionally, facial recognition technology can be used to search for missing persons, such as children or elderly individuals, and can assist in the identification of human remains.

Closed-circuit television (CCTV) cameras have become a common sight in many cities around the world, and law enforcement bodies have begun to use them as a tool for mass surveillance. This technology is based on the use of cameras that can capture images and videos of individuals in public spaces and transmit them to a central monitoring station. One of the main advantages of using CCTV cameras for mass surveillance is that they can help to deter crime. This is because the presence of cameras can make individuals think twice before committing a crime, as they know that they might be caught on camera. CCTV cameras can be used to monitor high-crime areas, such as city centers or public transportation systems, in order to identify and track suspects. Additional benefit of using CCTV cameras is that they can help to increase the efficiency of law enforcement. Cameras can provide real-time footage that can be used to track suspects and assist in the identification of suspects. CCTV cameras can also be used to monitor large crowds, such as at public events, to ensure public safety and to identify potential suspects or persons of interest.

There are, however, potential downsides to using facial recognition technology and CCTV cameras. One of the main concerns is that they may be used to violate individual privacy rights. There are also concerns that the technology could be used to target certain groups, such as people of color

or those with certain physical characteristics. Furthermore, the accuracy of facial recognition technology can be affected by factors such as lighting, angle, and facial expressions, which may lead to false positive or false negative identifications. The use of CCTV cameras for mass surveillance can lead to a feeling of being constantly monitored and can have a negative impact on mental health. In addition, the presence of CCTV cameras can lead to a chilling effect on free speech and freedom of assembly.

Facial recognition technology has the potential to be a valuable tool for law enforcement bodies in their efforts to identify suspects and solve crimes. It is critical to ensure that the technology is used in a way that respects individual privacy rights and does not lead to discrimination or bias. Measures must be taken to ensure the accuracy of the technology and to minimize the risk of false identifications, to ensure the protection of individuals' rights and to minimize the negative impact of surveillance on mental health and civil liberties. There should be a clear and transparent legal framework for the use of CCTV cameras for mass surveillance and a system of oversight and accountability to ensure that the technology is used in a responsible and ethical manner.

Among other relevant regulatory instruments, two documents stand out. The EU Law Enforcement Directive, also known as the Directive on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, is a piece of legislation adopted by the European Union in 2016. The Directive aims to protect personal data processed by EU law enforcement bodies in the context of preventing, investigating, detecting, or prosecuting criminal offenses. One of the main goals of the Directive is to ensure a high level of protection for individuals' personal data in the context of law enforcement activities. To achieve this, the Directive sets out a series of rules and principles for the processing of personal data, including the need for a legal basis for processing, transparency and fairness, and the right to access, rectify, and delete personal data.

The EU Draft Artificial Intelligence Act is a proposed piece of legislation that aims to regulate the use of artificial intelligence (AI) in the European Union. The Act, which is currently in the draft stage, seeks to ensure the safety and security of AI systems, as well as to protect individuals' rights and freedoms in relation to their use. One of the main goals of the Act is to ensure the safety and security of AI systems. This includes requirements for transparency, traceability, and accountability, as well as measures to ensure that AI systems are robust, reliable, and trustworthy. Additionally, the Act includes provisions for the testing and certification of AI systems, as well as for the reporting of incidents and accidents.

Real-time mass surveillance is an area that the EU Draft Artificial Intelligence Act is also addressing. The Act aims to regulate the use of AI systems for the purpose of mass surveillance, including the use of facial recognition technology, and to ensure that such systems are used in a way that respects individuals' rights and freedoms. This includes the requirement for a legal basis for the processing of data, the need for transparency and fairness, and the right to access, rectify, and delete data.